**Privacy Policy / Datenschutzerklärung**

Google

GOOGLE-DATENSCHUTZERKLÄRUNG

Wenn Sie unsere Dienste nutzen, vertrauen Sie uns Ihre Daten an. Wir sind uns bewusst, dass dies eine große Verantwortung ist und setzen alles daran, Ihre Daten zu schützen und zu gewährleisten, dass Sie die Kontrolle darüber behalten.

In dieser Datenschutzerklärung erfahren Sie, welche Daten von uns erhoben werden, welche Zwecke wir damit verfolgen und wie Sie Ihre Daten aktualisieren, verwalten, exportieren und löschen können.

Privatsphärecheck

Sie möchten Ihre Datenschutzeinstellungen ändern?

[Privatsphärecheck machen](https://myaccount.google.com/privacycheckup?utm_source=pp&utm_medium=Promo-in-product&utm_campaign=pp_intro&hl=de)

Wirksam ab dem 30. September 2020 | [Archivierte Versionen](https://policies.google.com/privacy/archive?hl=de) | [PDF herunterladen](https://www.gstatic.com/policies/privacy/pdf/20200930/r9u74aii/google_privacy_policy_de_eu.pdf)

Wir entwickeln eine Vielzahl von Diensten, die Millionen von Menschen Tag für Tag helfen, die Welt ganz neu zu entdecken und mit ihr zu interagieren. Zu unseren Diensten zählen:

* Google-Apps, -Websites und -Geräte, wie die Google-Suche, YouTube und Google Home
* Plattformen wie der Chrome-Browser und das Android-Betriebssystem
* Produkte, die in Apps und Websites von Drittanbietern integriert sind, wie Werbeanzeigen und das eingebettete Google Maps

Sie können die Datenschutzeinstellungen unserer Dienste auf vielfältige Weise verwalten. So haben Sie beispielsweise die Möglichkeit, sich für ein Google-Konto zu registrieren, wenn Sie Inhalte wie E-Mails und Fotos erstellen und verwalten oder relevantere Suchergebnisse erhalten möchten. Sie können auch zahlreiche Google-Dienste nutzen, ohne sich anzumelden oder ein Konto zu erstellen, beispielsweise wenn Sie die Google-Suche verwenden oder sich YouTube-Videos ansehen. Zusätzlich ist es möglich, in Chrome im Inkognitomodus privat im Web zu surfen. Für alle unsere Dienste können Sie Datenschutzeinstellungen festlegen und damit steuern, welche Daten wir erheben und wie diese verwendet werden.

Um Ihnen unsere Datenschutzerklärung möglichst verständlich zu machen, haben wir Beispiele, Videos und Definitionen für [Schlüsselbegriffe](https://policies.google.com/privacy/key-terms?hl=de#key-terms) angefügt. Wenn Sie dennoch Fragen dazu haben, [können Sie uns gern kontaktieren](https://support.google.com/policies?p=privpol_privts&hl=de).

VON GOOGLE ERHOBENE DATEN

Im Folgenden erklären wir Ihnen, welche Arten von Daten wir erheben, während Sie unsere Dienste nutzen

Wir erheben Daten, um allen unseren Nutzern bessere Dienste zur Verfügung zu stellen – von der Feststellung grundlegender Informationen wie zum Beispiel Ihrer Sprache bis hin zu komplexeren Fragen wie zum Beispiel [Werbung, die Sie besonders nützlich finden](https://policies.google.com/privacy?hl=de#footnote-useful-ads), den [Personen, mit denen Sie online am häufigsten zu tun haben](https://policies.google.com/privacy?hl=de#footnote-people-online), oder den YouTube-Videos, die Sie interessant finden. Welche Daten Google erhebt und wie diese verwendet werden hängt davon ab, wie Sie unsere Dienste nutzen und wie Sie Ihre Datenschutzeinstellungen verwalten.

Wenn Sie nicht in einem Google-Konto angemeldet sind, speichern wir die von uns erhobenen Daten mit [eindeutigen Kennungen](https://policies.google.com/privacy?hl=de#footnote-unique-id), die mit dem Browser, der App oder dem [Gerät](https://policies.google.com/privacy?hl=de#footnote-device) verknüpft sind, welche Sie verwenden. Damit können wir beispielsweise gewährleisten, dass Ihre Spracheinstellungen bei allen Browsersitzungen beibehalten werden.

Wenn Sie in einem Google-Konto angemeldet sind, erheben wir auch Daten, die wir in Ihrem Google-Konto speichern und als [personenbezogene Daten](https://policies.google.com/privacy?hl=de#footnote-personal-info) erachten.

Daten, die Sie uns bei der Nutzung unserer Dienste bereitstellen

Wenn Sie ein Google-Konto erstellen, geben Sie uns [personenbezogene Daten](https://policies.google.com/privacy?hl=de#footnote-personal-info), darunter Ihren Namen und ein Passwort. Sie können Ihrem Konto auch eine [Telefonnummer](https://policies.google.com/privacy?hl=de#footnote-phone-number) oder [Zahlungsinformationen](https://policies.google.com/privacy?hl=de#footnote-payment-info) hinzufügen. Selbst wenn Sie nicht bei einem Google-Konto angemeldet sind, können Sie uns Daten bereitstellen, etwa eine E-Mail-Adresse, um Benachrichtigungen zu unseren Diensten zu erhalten.

Wir erheben auch die Inhalte, die Sie bei der Nutzung unserer Dienste erstellen, hochladen oder von anderen erhalten. Dazu gehören beispielsweise E-Mails, die Sie verfassen und empfangen, Fotos und Videos, die Sie speichern, Dokumente und Tabellen, die Sie erstellen, und Kommentare, die Sie zu YouTube-Videos schreiben.

Daten, die wir bei der Nutzung unserer Dienste erheben

Ihre Apps, Browser und Geräte

Wir erheben Daten über die Apps, Browser und [Geräte](https://policies.google.com/privacy?hl=de#footnote-devices), die Sie beim Zugriff auf Google-Dienste verwenden. Das hilft uns, Funktionen wie automatische Produktupdates anzubieten oder Ihren Bildschirm zu dimmen, wenn Ihr Akku schwach ist.

Zu den von uns erhobenen Daten zählen [eindeutige Kennungen](https://policies.google.com/privacy?hl=de#footnote-unique-id), der Typ und die Einstellungen des Browsers, der Typ und die Einstellungen des Geräts, das Betriebssystem, Informationen zum Mobilfunknetz wie der Name des Mobilfunkanbieters und die Telefonnummer sowie die Versionsnummer der App. Wir erheben auch Daten über die Interaktion Ihrer Apps, Browser und Geräte mit unseren Diensten. Hierzu zählen u. a. die [IP-Adresse](https://policies.google.com/privacy?hl=de#footnote-ip), Absturzberichte, Systemaktivitäten sowie das Datum, die Uhrzeit und die Verweis-URL Ihrer Anfrage.

Wir erheben diese Daten, wenn ein Google-Dienst auf Ihrem Gerät unsere Server kontaktiert, beispielsweise wenn Sie eine App vom Play Store installieren oder wenn ein Dienst automatische Updates abfragt. Wenn Sie ein [Android-Gerät mit Google Apps](https://policies.google.com/privacy?hl=de#footnote-android-device) verwenden, kontaktiert Ihr Gerät regelmäßig die Google-Server, um Daten über Ihr Gerät und die Verbindung zu unseren Diensten bereitzustellen. Zu diesen Daten zählen beispielsweise der Typ Ihres Geräts, der Name des Mobilfunkanbieters, Absturzberichte und die von Ihnen installierten Apps.

Ihre Aktivitäten

Wir erheben in unseren Diensten Daten zu Ihren Aktivitäten. Diese Daten verwenden wir beispielsweise, um Ihnen ein YouTube-Video zu empfehlen, das Ihnen gefallen könnte. Unter anderem könnten folgende Aktivitätsdaten erhoben werden:

* Begriffe, nach denen Sie suchen
* Videos, die Sie sich ansehen
* [Inhalte und Werbeanzeigen, die Sie sich ansehen und mit denen Sie interagieren](https://policies.google.com/privacy?hl=de#footnote-content-views)
* Sprach- und Audiodaten bei Ihrer Nutzung von Audiofunktionen
* Kaufaktivitäten
* Personen, mit denen Sie kommunizieren oder Inhalte austauschen
* Aktivitäten auf Websites und Apps von Drittanbietern, die unsere Dienste nutzen
* Der Chrome-Browserverlauf, den Sie [mit Ihrem Google-Konto synchronisiert](https://policies.google.com/privacy?hl=de#footnote-chrome-sync) haben

Wenn Sie unsere [Dienste nutzen, um Anrufe zu tätigen und zu erhalten oder um Nachrichten zu senden und zu empfangen](https://policies.google.com/privacy?hl=de#footnote-calls-messages), erheben wir möglicherweise Telefonie-Informationen wie Ihre Telefonnummer, die Anrufernummer, die Nummer des Angerufenen, Weiterleitungsnummern, das Datum und die Uhrzeit von Anrufen und Nachrichten, die Dauer von Anrufen, Routing-Informationen und die Art der Anrufe.

Die in Ihrem Konto gespeicherten Aktivitätsdaten können Sie sich in Ihrem Google-Konto ansehen und sie dort auch verwalten.

[Zum Google-Konto](https://myaccount.google.com/?utm_source=pp&hl=de)

Ihre Standortdaten

Wenn Sie unsere Dienste nutzen, erheben wir Daten zu Ihrem Standort. Dadurch können wir Ihnen Funktionen wie Wegbeschreibungen für Ihren Wochenendausflug oder Spielzeiten von Kinofilmen in Ihrer Nähe anbieten.

Ihr Standort kann mit unterschiedlicher Genauigkeit bestimmt werden. Dazu verwenden wir:

* GPS
* [IP-Adresse](https://policies.google.com/privacy?hl=de#footnote-ip)
* [Sensordaten von Ihrem Gerät](https://policies.google.com/privacy?hl=de#footnote-sensor-data)
* [Informationen über Objekte in der Nähe Ihres Geräts](https://policies.google.com/privacy?hl=de#footnote-near-device), wie etwa WLAN-Zugriffspunkte, Funkmasten und Bluetooth-fähige Geräte

Die durch uns erhobenen Typen von Standortdaten hängen zum Teil von Ihren Geräte- und Kontoeinstellungen ab. Zum Beispiel können Sie mit der App "Einstellungen" in Ihrem Android-Gerät [die Standorterfassung Ihres Geräts aktivieren oder deaktivieren](https://support.google.com/accounts?p=privpol_location&hl=de). Wenn Sie eine private Karte mit Orten erstellen möchten, die Sie mit Ihren angemeldeten Geräten besuchen, können Sie auch den [Standortverlauf](https://support.google.com/accounts?p=privpol_lochistory&hl=de) aktivieren.

In manchen Fällen erhebt Google auch Daten über Sie aus [öffentlich zugänglichen Quellen](https://policies.google.com/privacy?hl=de#footnote-sources). Wenn beispielsweise Ihr Name in Ihrer lokalen Zeitung erscheint, kann die Google-Suchmaschine diesen Artikel indexieren und anderen Personen zeigen, wenn sie nach Ihrem Namen suchen. Unter Umständen erhalten wir auch Daten über Sie von vertrauenswürdigen Partnern . Dazu zählen Marketingpartner, die uns Daten über potenzielle Kunden unserer Geschäftsdienste bereitstellen und Sicherheitspartner, die uns Daten liefern, mit denen wir uns [vor Missbrauch schützen](https://policies.google.com/privacy?hl=de#footnote-against-abuse) können. Wir erhalten auch Daten von [Werbetreibenden, damit wir in deren Namen Werbung und Recherchedienste bereitstellen können](https://policies.google.com/privacy?hl=de#footnote-ad-services).

Zum Erheben und Speichern von Daten verwenden wir verschiedene Technologien. Dazu zählen [Cookies](https://policies.google.com/privacy?hl=de#footnote-cookies), [Pixel-Tags](https://policies.google.com/privacy?hl=de#footnote-pixel), die lokale Speicherung wie etwa [Browser-Webspeicher](https://policies.google.com/privacy?hl=de#footnote-browser-storage) oder [Anwendungsdaten-Caches](https://policies.google.com/privacy?hl=de#footnote-application-data-cache), Datenbanken und [Serverprotokolle](https://policies.google.com/privacy?hl=de#footnote-server-logs).

GRÜNDE FÜR DIE DATENERHEBUNG DURCH GOOGLE

Wir verwenden Daten zur Verbesserung unserer Dienste

Wir nutzen die von uns im Rahmen unserer Dienste erhobenen Daten für folgende Zwecke:

Bereitstellung unserer Dienste

Wir nutzen Ihre Daten zur [Bereitstellung unserer Dienste](https://policies.google.com/privacy?hl=de#footnote-deliver-services). Hierzu zählen beispielsweise die Verarbeitung Ihrer Suchbegriffe, um Suchergebnisse einzublenden, oder das Vorschlagen von Empfängern aus Ihren Kontakten, wenn Sie Inhalte teilen möchten.

Wartung und Verbesserung unserer Dienste

Wir verwenden Ihre Daten, [um zu gewährleisten, dass unsere Dienste ordnungsgemäß funktionieren](https://policies.google.com/privacy?hl=de#footnote-ensure-working). Beispielsweise verwenden wir sie zur Überprüfung von Störungen oder zur Beseitigung von Problemen, die Sie uns gemeldet haben. Außerdem nutzen wir Ihre Daten, um [unsere Dienste zu verbessern](https://policies.google.com/privacy?hl=de#footnote-make-improvements). Dazu zählt beispielsweise die Feststellung, welche Suchbegriffe am häufigsten falsch geschrieben werden, damit wir die in unseren Diensten verwendete Rechtschreibprüfung verbessern können.

Entwicklung neuer Dienste

Wir nutzen die im Rahmen unserer bestehenden Dienste erhobenen Daten zur Entwicklung neuer Dienste. Beispielsweise halfen uns Erkenntnisse darüber, wie Personen Fotos in Picasa, der ersten Foto-App von Google, organisiert haben, bei der Entwicklung von Google Fotos.

Bereitstellung personalisierter Dienste, einschließlich Inhalte und Werbeanzeigen

Wir nutzen die von uns erhobenen Daten zur Personalisierung unserer Dienste. Dazu zählen die Bereitstellung von Empfehlungen, von personalisierten Inhalten und [von personalisierten Suchergebnissen](https://policies.google.com/privacy?hl=de#footnote-customized-search). Beispielsweise erhalten Sie im [Sicherheitscheck](https://myaccount.google.com/security-checkup?utm_source=pp&hl=de) Sicherheitstipps, die auf Ihre persönliche Nutzung von Google-Produkten zugeschnitten sind. Google Play nutzt Daten, etwa über Apps, die Sie installiert haben, und Videos, die Sie sich auf YouTube angesehen haben, um neue Apps zu empfehlen, die Ihnen gefallen könnten.

Abhängig von Ihren Einstellungen zeigen wir Ihnen möglicherweise auch auf Ihre Interessen abgestimmte [personalisierte Werbung](https://policies.google.com/privacy?hl=de#footnote-personalized-ads). Wenn Sie beispielsweise nach Mountainbikes suchen, kann Ihnen eine Werbeanzeige zu Sportausrüstung eingeblendet werden, wenn Sie auf einer Website surfen, auf der von Google ausgelieferte Werbeanzeigen erscheinen. In den Einstellungen für Werbung können Sie selbst festlegen, welche Daten wir zum Schalten von Anzeigen verwenden können.

* Wir zeigen Ihnen keine personalisierte Werbung, die auf [sensiblen Kategorien](https://policies.google.com/privacy?hl=de#footnote-sensitive-categories), wie der ethnischen Zugehörigkeit, Religion, sexuellen Orientierung oder Gesundheit beruht.
* Wir geben Daten, durch die Sie persönlich identifizierbar sind, wie beispielsweise Ihren Namen oder Ihre E-Mail-Adresse, nur dann an Werbetreibende weiter, wenn Sie uns dazu auffordern. Wenn Sie beispielsweise Werbung für einen Blumenladen in Ihrer Nähe sehen und die Schaltfläche "Zum Anrufen tippen" auswählen, verbinden wir Ihren Anruf und geben Ihre Telefonnummer möglicherweise an den Blumenladen weiter.

[Zu den Einstellungen für Werbung](https://adssettings.google.com/?utm_source=pp&hl=de)

Messung der Leistung

Wir nutzen die Daten zur Analyse und Messung, um zu verstehen, wie unsere Dienste verwendet werden. Beispielsweise analysieren wir Daten über Ihre Besuche auf unseren Websites, um das Design unserer Produkte zu optimieren. Zusätzlich nutzen wir Daten der Werbeanzeigen, mit denen Sie interagieren, um Werbetreibenden ein besseres Verständnis ihrer Werbekampagnen zu ermöglichen. Dazu nutzen wir verschiedene Tools, wie z. B. Google Analytics. Wenn Sie Websites besuchen, auf denen Google Analytics eingesetzt wird, werden Google und der Google Analytics-Kunde gegebenenfalls [Daten über Ihre Aktivitäten auf dieser Website mit Aktivitäten auf anderen Websites verknüpfen](https://policies.google.com/privacy?hl=de#footnote-link-info), auf denen ebenfalls unsere Werbedienste genutzt werden.

Kommunikation mit Ihnen

Wir nutzen die von uns erhobenen Daten, wie Ihre E-Mail-Adresse, um uns direkt mit Ihnen in Verbindung zu setzen. So könnten wir Ihnen beispielsweise eine Benachrichtigung senden, wenn wir verdächtige Aktivitäten feststellen, wie einen Versuch, sich von einem ungewöhnlichen Standort aus in Ihrem Google-Konto anzumelden. Außerdem könnten wir Sie auch über bevorstehende Änderungen oder Verbesserungen in Bezug auf unsere Dienste informieren. Und wenn Sie Google kontaktieren, zeichnen wir Ihre Anfrage auf, um Ihnen bei der Lösung etwaiger Probleme behilflich zu sein.

Schutz von Google, unserer Nutzer und der Öffentlichkeit

Wir nutzen Daten, um die [Sicherheit und Zuverlässigkeit](https://policies.google.com/privacy?hl=de#footnote-safety-reliability) unserer Dienste zu verbessern. Dazu zählen das Erkennen, Verhindern und Bekämpfen von Betrug, Missbrauch, Sicherheitsrisiken und technischen Problemen, die Google, unseren Nutzern oder der Öffentlichkeit schaden könnten.

Um Ihre Daten zu diesen Zwecken zu verarbeiten, verwenden wir verschiedene Technologien. Wir nutzen automatisierte Systeme, die Ihre Inhalte analysieren, sodass wir Ihnen personalisierte Suchergebnisse, personalisierte Werbung oder andere Funktionen bereitstellen können, die auf Ihre Nutzung unserer Dienste zugeschnitten sind. Zusätzlich analysieren wir Ihre Inhalte, damit wir [Missbrauch erkennen können](https://policies.google.com/privacy?hl=de#footnote-detect-abuse), wie Spam, Malware und illegale Inhalte. Wir verwenden auch [Algorithmen](https://policies.google.com/privacy?hl=de#footnote-algorithm), um Muster in Daten zu erkennen. Google Übersetzer hilft beispielsweise Personen, über Sprachbarrieren hinweg zu kommunizieren, indem der Dienst geläufige Sprachmuster in Sätzen erkennt, die übersetzt werden sollen.

Unter Umständen werden die durch uns erhobenen Daten zu den oben beschriebenen Zwecken [dienst- und geräteübergreifend kombiniert](https://policies.google.com/privacy?hl=de#footnote-combine-info). Wenn Sie sich beispielsweise Videos von Gitarrenspielern auf YouTube ansehen, kann eine Werbeanzeige für Gitarrenunterricht auf einer Website geschaltet werden, auf der unsere Anzeigenprodukte verwendet werden. Je nach Ihren Kontoeinstellungen könnten [Ihre Aktivitäten auf anderen Websites und in Apps](https://policies.google.com/privacy?hl=de#footnote-other-sites) mit Ihren personenbezogenen Daten verknüpft werden, um die Dienste von Google und die von Google ausgelieferten Werbeanzeigen zu verbessern.

Wenn andere Nutzer bereits über Ihre E-Mail-Adresse oder andere Sie identifizierende Daten verfügen, zeigen wir diesen Nutzern möglicherweise die öffentlich sichtbaren Daten Ihres Google-Kontos an, wie Ihren Namen und Ihr Foto. Damit können andere Personen beispielsweise eine von Ihnen stammende E-Mail identifizieren.

Bevor wir Daten zu anderen als den in dieser Datenschutzerklärung aufgeführten Zwecken nutzen, bitten wir Sie um Ihre Einwilligung.

DATENSCHUTZEINSTELLUNGEN

Sie haben Entscheidungsmöglichkeiten in Bezug auf die durch uns erhobenen Daten und ihre Verwendung

In diesem Abschnitt werden die wichtigsten Einstellungen beschrieben, mit denen Sie Ihre Privatsphäre in unseren Diensten verwalten können. Sie können auch den [Privatsphärecheck](https://myaccount.google.com/privacycheckup?utm_source=pp&utm_medium=Promo-in-product&utm_campaign=pp_body&hl=de) verwenden, um wichtige Datenschutzeinstellungen zu überprüfen und anzupassen. Zusätzlich zu diesen Tools bieten wir auch spezifische Datenschutzeinstellungen in unseren Produkten. Mehr dazu erfahren Sie in unserem [Leitfaden zum Datenschutz in Google-Produkten](https://policies.google.com/technologies/product-privacy?hl=de).

[Zum Privatsphärecheck](https://myaccount.google.com/privacycheckup?utm_source=pp&utm_medium=Promo-in-product&utm_campaign=pp_body&hl=de)

Daten verwalten, überprüfen und aktualisieren

Wenn Sie angemeldet sind, können Sie Ihre Daten jederzeit in den von Ihnen verwendeten Diensten überprüfen und aktualisieren. Beispielsweise ermöglichen Ihnen Fotos und Drive die Verwaltung bestimmter auf Google gespeicherter Inhaltstypen.

Wir stellen Ihnen auch einen Ort zur Verfügung, an dem Sie die in Ihrem Google-Konto gespeicherten Daten überprüfen und deren Speicherung steuern können. Ihr [Google-Konto](https://myaccount.google.com/?hl=de) beinhaltet:

Datenschutzeinstellungen

**Aktivitätseinstellungen**

Hier können Sie festlegen, welche Arten von Aktivitäten in Ihrem Konto gespeichert werden sollen. So können Sie beispielsweise den Standortverlauf aktivieren, wenn Sie Verkehrsmeldungen für Ihren täglichen Weg zur Arbeit erhalten möchten, oder Ihren YouTube-Wiedergabeverlauf speichern, um bessere Videoempfehlungen zu erhalten.

[Aktivitätseinstellungen aufrufen](https://myaccount.google.com/activitycontrols?utm_source=pp&hl=de)

**Einstellungen für Werbung**

Hier können Sie Ihre Einstellungen zu Werbeanzeigen verwalten, die auf Google sowie auf Websites und in Apps im Rahmen einer [Partnerschaft mit Google](https://policies.google.com/privacy?hl=de#footnote-partner) von Google ausgeliefert werden. Sie können Ihre Interessen verändern, auswählen, ob Ihre personenbezogenen Daten verwendet werden sollen, um sich relevantere Werbung präsentieren zu lassen, und bestimmte Werbedienste aktivieren oder deaktivieren.

[Zu den Einstellungen für Werbung](https://adssettings.google.com/?utm_source=pp&hl=de)

**Über mich**

Hier können Sie festlegen, was andere über Sie in Google-Diensten sehen können.

[Zu "Über mich"](https://myaccount.google.com/profile?utm_source=pp&hl=de)

**Soziale Empfehlungen**

Hier können Sie auswählen, ob Ihr Name und Ihr Foto neben Ihren Aktivitäten wie Rezensionen und Empfehlungen in Werbeanzeigen erscheinen sollen.

[Zu "Soziale Empfehlungen"](https://myaccount.google.com/shared-endorsements?utm_source=pp&hl=de)

Möglichkeiten zur Überprüfung und Aktualisierung Ihrer Daten

**Meine Aktivitäten**

In "Meine Aktivitäten" können Sie überprüfen und festlegen, welche Daten bei der Verwendung von Google-Diensten erstellt werden, wie etwa vergangene Suchanfragen oder Besuche auf Google Play. Sie können sich die Inhalte nach Datum und Thema sortiert ansehen und Teile Ihrer Aktivitäten oder alle löschen.

[Zu "Meine Aktivitäten"](https://myactivity.google.com/myactivity?utm_source=pp&hl=de)

**Google Dashboard**

Google Dashboard ermöglicht Ihnen die Verwaltung von Daten, die mit bestimmten Produkten verknüpft sind.

[Zu Google Dashboard](https://myaccount.google.com/dashboard?utm_source=pp&hl=de)

**Ihre personenbezogenen Daten**

Hier können Sie Ihre Kontaktdaten wie Ihren Namen, Ihre E-Mail-Adresse und Ihre Telefonnummer verwalten.

[Zu den personenbezogenen Daten](https://myaccount.google.com/personal-info?utm_source=pp&hl=de)

Wenn Sie abgemeldet sind, können Sie Daten verwalten, die mit Ihrem Browser oder Gerät verknüpft sind, z. B.:

* Personalisierte Suche: [Hier können Sie auswählen](https://www.google.com/history/optout?utm_source=pp&hl=de), ob Ihnen anhand Ihrer Suchaktivitäten relevantere Ergebnisse und Empfehlungen bereitgestellt werden sollen.
* YouTube-Einstellungen: Hier können Sie Ihren [YouTube-Suchverlauf](https://www.youtube.com/feed/history/search_history?utm_source=pp&hl=de) und Ihren [YouTube-Wiedergabeverlauf](https://www.youtube.com/feed/history?utm_source=pp&hl=de) pausieren und löschen.
* Einstellungen für Werbung: Hier können Sie [Ihre Einstellungen für Werbeanzeigen verwalten](https://adssettings.google.com/?utm_source=pp&hl=de), die Ihnen auf Google und Websites sowie in Apps von Google-Anzeigenpartnern präsentiert werden.

Daten exportieren, entfernen und löschen

Sie können eine Kopie Ihrer Inhalte aus Ihrem Google-Konto exportieren, um diese zu sichern oder sie mit einem anderen Dienst als den von Google zu nutzen.

[Daten exportieren](https://takeout.google.com/?utm_source=pp&hl=de)

Sie können auch gemäß dem anwendbaren Recht [eine Anfrage zum Entfernen von Inhalten](https://support.google.com/legal?p=privpol_remove&hl=de) aus bestimmten Google-Diensten stellen.

Zum Löschen Ihrer Daten haben Sie folgende Möglichkeiten:

* Inhalte aus [bestimmten Google-Diensten](https://policies.google.com/privacy?hl=de#footnote-delete-specific) löschen
* Bestimmte Elemente in Ihrem Konto unter Verwendung von [Meine Aktivitäten](https://myactivity.google.com/?utm_source=pp&hl=de) suchen und dann löschen
* [Bestimmte Google-Produkte](https://myaccount.google.com/deleteservices?utm_source=pp&hl=de) einschließlich Ihrer mit diesen Produkten verknüpften Daten löschen
* [Gesamtes Google-Konto löschen](https://myaccount.google.com/deleteaccount?utm_source=pp&hl=de)

[Daten löschen](https://myaccount.google.com/delete-services-or-account?utm_source=pp&hl=de)

Und schließlich können Sie über den [Kontoinaktivität-Manager](https://myaccount.google.com/inactive?utm_source=pp&hl=de) auch einer anderen Person Zugriff zu Teilen Ihres Google-Kontos gewähren, falls Sie unerwarteterweise nicht in der Lage sind, Ihr Konto zu verwenden.

Es gibt auch andere Möglichkeiten festzulegen, welche Daten von Google erhoben werden dürfen, und zwar unabhängig davon, ob Sie in einem Google-Konto angemeldet sind oder nicht. Hierzu zählen:

* Browsereinstellungen: Ihr Browser lässt sich beispielsweise so konfigurieren, dass angezeigt wird, wenn von Google ein [Cookie](https://policies.google.com/privacy?hl=de#footnote-cookies) in Ihrem Browser gesetzt wurde. Ihr Browser lässt sich auch so konfigurieren, dass alle Cookies von einer bestimmten Domain oder allen Domains blockiert werden. Beachten Sie aber, dass Cookies erforderlich sind, [damit unsere Dienste ordnungsgemäß funktionieren](https://policies.google.com/privacy?hl=de#footnote-rely-on-cookies) und etwa Ihre Spracheinstellungen gespeichert werden können.
* Geräteeinstellungen: Ihr Gerät verfügt möglicherweise über Steuerelemente, mit denen Sie festlegen können, welche Daten wir erheben. So können Sie beispielsweise auf Ihrem Android-Gerät [Standorteinstellungen anpassen](https://support.google.com/websearch?p=privpol_locserp&hl=de).

DATENWEITERGABE

Datenweitergabe durch Sie

In vielen unserer Dienste können Sie Daten mit anderen Personen teilen. Sie bestimmen in diesem Fall, wie dabei vorgegangen werden soll. Beispielsweise können Sie entscheiden, welche Ihrer Videos auf YouTube öffentlich geteilt werden und welche vertraulich bleiben sollen. Bedenken Sie, dass, wenn Sie Daten öffentlich teilen, Suchmaschinen, einschließlich der Google-Suche, möglicherweise auf diese Daten zugreifen können.

Wenn Sie angemeldet sind und mit Google-Diensten interagieren, z. B. wenn Sie Kommentare zu einem YouTube-Video verfassen oder eine App bei Play rezensieren, werden Ihr Name und Ihr Foto neben Ihrer Aktivität angezeigt. Diese Daten werden wir gegebenenfalls [entsprechend Ihren Einstellungen für "Soziale Empfehlungen"](https://support.google.com/accounts?p=privpol_endorse&hl=de) auch in Werbeanzeigen veröffentlichen.

Datenweitergabe durch Google

Wir geben personenbezogene Daten an Unternehmen, Organisationen oder Personen außerhalb von Google nur in folgenden Fällen weiter:

Mit Ihrer Einwilligung

Wir geben personenbezogene Daten außerhalb von Google weiter, wenn wir Ihre Einwilligung dazu haben. Wenn Sie beispielsweise [Google Home verwenden, um eine Tischreservierung vorzunehmen](https://support.google.com/googlehome?p=privpol_homedata&hl=de), holen wir Ihre Einwilligung ein, bevor wir dem Restaurant Ihren Namen oder Ihre Telefonnummer weitergeben. Vor der Weitergabe von [vertraulichen personenbezogenen Daten](https://policies.google.com/privacy?hl=de#footnote-sensitive-info) holen wir Ihre ausdrückliche Einwilligung ein.

Im Falle von Domain-Administratoren

Wenn Sie Mitglied einer Bildungseinrichtung oder Mitarbeiter einer Organisation sind, die Google-Dienste nutzt, haben der [Domainadministrator](https://support.google.com/a?p=privpol_admin&hl=de) und Reseller, die Ihr Konto verwalten, Zugriff auf Ihr Google-Konto. Diese haben folgende Möglichkeiten:

* Auf die in Ihrem Konto gespeicherten Daten zugreifen und diese speichern, z. B. Ihre E-Mail
* Statistiken zu Ihrem Konto ansehen, z. B. wie viele Apps Sie installieren
* Das Passwort für Ihr Konto ändern
* Den Zugriff auf Ihr Konto sperren oder beenden
* Ihre Kontodaten abrufen, um anwendbare Gesetze, Vorschriften und gerichtliche Verfahren einzuhalten oder einer vollstreckbaren behördlichen Anordnung nachzukommen
* Ihre Möglichkeiten einschränken, Daten oder Datenschutzeinstellungen zu löschen oder zu bearbeiten

Für die Verarbeitung durch andere Stellen

Wir stellen personenbezogene Daten unseren [verbundenen Unternehmen](https://policies.google.com/privacy?hl=de#footnote-affiliates), anderen vertrauenswürdigen Unternehmen oder Personen zur Verfügung, die diese in unserem Auftrag verarbeiten. Dies geschieht auf der Grundlage unserer Weisungen und im Einklang mit unserer Datenschutzerklärung sowie anderen geeigneten Vertraulichkeits- und Sicherheitsmaßnahmen. Beispielsweise nutzen wir Dienstanbieter zur Unterstützung beim Kundensupport.

Aus rechtlichen Gründen

Wir geben personenbezogene Daten an Stellen außerhalb von Google weiter, wenn wir nach Treu und Glauben davon ausgehen dürfen, dass der Zugriff auf diese Daten oder ihre Nutzung, Aufbewahrung oder Offenlegung vernünftigerweise notwendig ist, um folgende Zwecke zu erfüllen:

* Geltende Gesetze, Vorschriften oder [gerichtliche Verfahren einzuhalten oder einer vollstreckbaren behördlichen Anordnung nachzukommen](https://policies.google.com/privacy?hl=de#footnote-legal). In unserem [Transparenzbericht](https://transparencyreport.google.com/user-data/overview?hl=de) veröffentlichen wir Daten über die Anzahl und die Art der Anfragen, die wir von Behörden erhalten.
* Geltende Nutzungsbedingungen durchzusetzen, einschließlich der Untersuchung möglicher Verstöße.
* Betrug, Sicherheitsmängel oder technische Probleme aufzudecken, zu verhindern oder anderweitig zu bekämpfen.
* Die Rechte, das Eigentum oder die Sicherheit von Google, unserer Nutzer oder der Öffentlichkeit vor Schaden zu schützen, soweit gesetzlich zulässig oder erforderlich.

Wir geben möglicherweise [nicht personenbezogene Daten](https://policies.google.com/privacy?hl=de#footnote-info) an die Öffentlichkeit und unsere Partner, beispielsweise an Publisher, Werbetreibende, Entwickler oder Rechteinhaber, weiter. Beispielsweise veröffentlichen wir Daten, [um Trends bezüglich der allgemeinen Nutzung unserer Dienste aufzuzeigen](https://policies.google.com/privacy?hl=de#footnote-trends). Darüber hinaus erlauben wir [bestimmten Partnern](https://policies.google.com/privacy?hl=de#footnote-specific-partners), Daten von Ihrem Browser oder Gerät unter Verwendung ihrer eigenen Cookies oder ähnlicher Technologien zu Werbe- und Messzwecken zu erheben.

Falls Google an einem Unternehmenszusammenschluss, einem Unternehmenserwerb oder einem Verkauf von Vermögensgegenständen beteiligt ist, werden wir weiterhin dafür sorgen, die Vertraulichkeit Ihrer personenbezogenen Daten sicherzustellen. Zusätzlich werden wir betroffene Nutzer benachrichtigen, bevor personenbezogene Daten übermittelt oder Gegenstand einer anderen Datenschutzerklärung werden.

GEWÄHRLEISTUNG DER DATENSICHERHEIT

Wir integrieren Sicherheitsfunktionen in unsere Dienste, um Ihre Daten zu schützen

Alle Google-Produkte sind mit starken Sicherheitsfunktionen ausgestattet, die Ihre Daten fortwährend schützen. Die Erkenntnisse, die wir durch die Bereitstellung unserer Dienste gewinnen, helfen uns, Bedrohungen der Sicherheit automatisch abzufangen und zu verhindern, dass Sie mit solchen konfrontiert werden. Wenn wir tatsächlich ein Risiko erkennen, von dem Sie unserer Meinung nach erfahren sollten, benachrichtigen wir Sie und schlagen Ihnen Maßnahmen vor, um sich besser zu schützen.

Wir bemühen uns intensiv darum, Sie und Google vor unbefugtem Zugriff auf Daten oder vor unbefugter Veränderung, Offenlegung oder Vernichtung von Daten zu schützen. Unsere Maßnahmen umfassen Folgendes:

* Wir verschlüsseln Ihre Daten, um sie während der Übertragung zu schützen.
* Wir bieten eine Vielzahl von Sicherheitsfunktionen, wie [Safe Browsing](https://safebrowsing.google.com/?utm_source=pp&hl=de), Sicherheitscheck und die [Bestätigung in zwei Schritten](https://www.google.com/landing/2step/?utm_source=pp&hl=de), um Ihnen zu helfen, Ihr Konto zu schützen.
* Wir überprüfen laufend unsere Praktiken zur Erhebung, Speicherung und Verarbeitung von Daten, einschließlich der physischen Sicherheitsmaßnahmen, um unsere Systeme vor unbefugtem Zugriff zu schützen.
* Der Zugriff auf personenbezogene Daten wird durch uns beschränkt und nur Mitarbeitern, Auftragnehmern und Kundenservicemitarbeitern von Google gewährt, die diese Daten für die weitere Datenverarbeitung unbedingt benötigen. Alle Personen mit diesen Zugriffsrechten sind strengen Vertraulichkeitsverpflichtungen unterworfen und können disziplinarischen Maßnahmen unterzogen oder entlassen werden, falls sie diese Verpflichtungen nicht einhalten.

LÖSCHEN UND EXPORTIEREN IHRER DATEN

Sie können Ihre Daten jederzeit exportieren oder aus Ihrem Google-Konto löschen.

Sie können eine Kopie Ihrer Inhalte aus Ihrem Google-Konto exportieren, um diese zu sichern oder sie mit einem anderen Dienst als den von Google zu nutzen.

[Daten exportieren](https://takeout.google.com/?utm_source=pp&hl=de)

Zum Löschen Ihrer Daten haben Sie folgende Möglichkeiten:

* Inhalte aus [bestimmten Google-Diensten](https://policies.google.com/privacy?hl=de#footnote-delete-specific) löschen
* Bestimmte Elemente in Ihrem Konto unter Verwendung von [Meine Aktivitäten](https://myactivity.google.com/?utm_source=pp&hl=de) suchen und dann löschen
* [Bestimmte Google-Produkte](https://myaccount.google.com/deleteservices?utm_source=pp&hl=de) einschließlich Ihrer mit diesen Produkten verknüpften Daten löschen
* [Gesamtes Google-Konto löschen](https://myaccount.google.com/deleteaccount?utm_source=pp&hl=de)

[Daten löschen](https://myaccount.google.com/delete-services-or-account?utm_source=pp&hl=de)

AUFBEWAHRUNG IHRER INFORMATIONEN

Wir speichern erhobene Daten über verschiedene Zeiträume, abhängig davon, um welche Daten es sich handelt, wie wir sie nutzen und wie Sie Ihre Einstellungen konfigurieren:

* Einige Daten können Sie jederzeit löschen, beispielsweise selbst erstellte oder hochgeladene Inhalte. Darüber hinaus können Sie in Ihrem Konto gespeicherte [Informationen zu Ihren Aktivitäten](https://myactivity.google.com/myactivity?hl=de) löschen oder [festlegen, dass diese nach einer bestimmten Zeit automatisch gelöscht werden](https://support.google.com/accounts/answer/465?authuser=0&hl=de#auto-delete).
* Andere Daten werden nach einer bestimmten Zeit automatisch gelöscht oder anonymisiert, etwa [Werbedaten](https://policies.google.com/technologies/ads?hl=de) in Serverprotokollen.
* Einige Daten, etwa dazu, wie oft Sie unsere Dienste nutzen, speichern wir, bis Sie Ihr Google-Konto löschen.
* Einige Daten speichern wir für längere Zeit, wenn dies aus legitimen geschäftlichen oder rechtlichen Gründen erforderlich ist. Diese Gründe können Sicherheit, Betrugs- und Missbrauchsabwehr oder eine Dokumentationspflicht im Finanzbereich sein.

Wenn Sie Daten löschen, beginnen wir mit einem Datenlöschvorgang, um dafür zu sorgen, dass die Daten sicher und vollständig von unseren Servern entfernt werden oder nur in anonymisierter Form gespeichert bleiben. Wir bemühen uns, Daten mithilfe unserer Dienste davor zu schützen, irrtümlich oder mutwillig gelöscht zu werden. Aus diesem Grund kann es zwischen der von Ihnen durchgeführten Löschung von Inhalten und dem Zeitpunkt, zu dem Kopien aus unseren aktiven Systemen und Sicherungssystemen gelöscht werden, zu Verzögerungen kommen.

Weitere Informationen zur Dauer der Datenspeicherung bei Google und Angaben dazu, wie lange es dauert, bis wir Ihre Informationen löschen, [finden Sie hier](https://policies.google.com/technologies/retention?hl=de).

COMPLIANCE UND ZUSAMMENARBEIT MIT REGIERUNGSBEHÖRDEN

Wir überprüfen die vorliegende Datenschutzerklärung regelmäßig und verarbeiten Ihre Daten entsprechend dieser Datenschutzerklärung.

Datenübermittlung

Wir betreiben [Server auf der ganzen Welt](https://policies.google.com/privacy?hl=de#footnote-servers). Deshalb können Ihre Daten auf Servern verarbeitet werden, die außerhalb des Landes liegen, in dem Sie leben. Datenschutzgesetze sind von Land zu Land unterschiedlich und einige bieten mehr Schutz als andere. Unabhängig davon, wo Ihre Daten verarbeitet werden, wenden wir grundsätzlich dieselben, in der Datenschutzerklärung beschriebenen Schutzmaßnahmen an. Ferner halten wir bestimmte [rechtliche Rahmenbedingungen](https://policies.google.com/privacy/frameworks?hl=de) zu Datenübermittlungen ein.

Sobald wir formale schriftliche Beschwerden erhalten, nehmen wir mit der Person, die die Beschwerde eingereicht hat, Kontakt auf. Wir arbeiten mit den jeweils zuständigen Regulierungsbehörden einschließlich der lokalen Datenschutzaufsichtsbehörden zusammen, um alle Beschwerden bezüglich der Übermittlung Ihrer Daten beizulegen, die wir nicht direkt mit Ihnen klären können.

Anforderungen in Europa

Wenn das Datenschutzrecht der Europäischen Union (EU) oder Großbritanniens für die Verarbeitung Ihrer Daten Anwendung findet, stellen wir Ihnen die in dieser Datenschutzerklärung beschriebenen Steuerungsmöglichkeiten zur Verfügung, damit Sie Ihr Recht ausüben können, Auskunft über Ihre Daten zu erhalten, sie zu aktualisieren, zu löschen und deren Verarbeitung einzuschränken. Darüber hinaus haben Sie das Recht, der Verarbeitung Ihrer Daten zu widersprechen oder Ihre Daten in einen anderen Dienst zu exportieren.

Bei Nutzern, die ihren gewöhnlichen Aufenthalt im Europäischen Wirtschaftsraum oder der Schweiz haben, ist Google Ireland Limited der für Ihre Daten zuständige Verantwortliche, sofern dies in den Datenschutzhinweisen eines bestimmten Dienstes nicht anders angegeben ist. Google Ireland Limited ist demnach das mit Google verbundene Unternehmen, welches für die Verarbeitung Ihrer Daten und die Einhaltung der anwendbaren Datenschutzgesetze verantwortlich ist.

Wir verarbeiten Ihre Daten zu den in dieser Datenschutzerklärung beschriebenen Zwecken auf der Basis der folgenden rechtlichen Grundlagen:

Mit Ihrer Einwilligung

Wir bitten Sie um Ihre Einwilligung zur Verarbeitung Ihrer Daten für bestimmte Zwecke und Sie haben das Recht, Ihre Einwilligung jederzeit zu widerrufen. Beispielsweise holen wir Ihre Einwilligung ein, um Ihnen personalisierte Dienste anbieten zu können, wie z. B. Werbung auf Grundlage Ihrer Interessen. Auch für die Erhebung Ihrer Sprach- und Audioaktivitäten zur Spracherkennung ist Ihre Einwilligung erforderlich. Diese Einstellungen können Sie in Ihrem [Google-Konto](https://myaccount.google.com/?hl=de) verwalten.

Aus berechtigten Interessen

Wir verarbeiten Ihre Daten, soweit wir oder [Dritte](https://policies.google.com/privacy?hl=de#footnote-third-parties) ein berechtigtes Interessen daran haben, dies zu tun. Dabei wenden wir [geeignete Maßnahmen](https://policies.google.com/privacy?hl=de#footnote-safeguards) zum Schutz Ihrer Daten an. Dies bedeutet, dass wir Ihre Daten u. a. für Folgendes verarbeiten:

* Bereitstellung, Wartung und Verbesserung unserer Dienste, um die Anforderungen unserer Nutzer zu erfüllen
* Entwicklung neuer Produkte und Funktionen, die für unsere Nutzer hilfreich sind
* Einblicke darüber, wie Personen unsere Dienste nutzen, um die Leistung unserer Dienste [zu gewährleisten und zu verbessern](https://policies.google.com/privacy?hl=de#footnote-improve)
* [Personalisierung unserer Dienste](https://policies.google.com/privacy?hl=de#footnote-customizing), um Ihnen ein besseres Nutzererlebnis zu bieten
* Marketing, um Nutzer über unsere Dienste zu informieren
* Werbung, um viele unserer Dienste kostenlos zur Verfügung stellen zu können (bei personalisierter Werbung holen wir Ihre Einwilligung ein)
* Aufdecken, Verhindern oder anderweitiges Bekämpfen von Betrug, Sicherheitsmängeln oder technischen Problemen
* Schutz der Rechte, des Eigentums oder der Sicherheit von Google, unserer Nutzer oder der Öffentlichkeit vor Schaden, soweit dies gesetzlich zulässig oder erforderlich ist, einschließlich der Offenlegung von Informationen gegenüber Behörden
* Durchführen von Recherchen, mit der unsere Dienste für unsere Nutzer verbessert werden und die für die Öffentlichkeit von Vorteil sind
* Einhalten von Verpflichtungen gegenüber unseren Partnern wie Entwicklern und Rechteinhabern
* Durchsetzen rechtlicher Forderungen, einschließlich der Untersuchung möglicher Verletzungen anwendbarer Nutzungsbedingungen

Bei der Bereitstellung eines Dienstes

Wir verarbeiten Ihre Daten, um Ihnen einen Dienst bereitzustellen, den Sie im Rahmen eines Vertrags angefordert haben. Beispielsweise verarbeiten wir Ihre Zahlungsinformationen, wenn Sie zusätzlichen Speicherplatz für Google Drive kaufen.

Bei der Erfüllung rechtlicher Verpflichtungen

Wir verarbeiten Ihre Daten, wenn wir dazu eine rechtliche Verpflichtung haben, z. B. im Rahmen eines [gerichtlichen Verfahrens oder eines vollstreckbaren behördlichen Ersuchens](https://policies.google.com/privacy?hl=de#footnote-legal).

Wenn Sie Fragen haben, [können Sie sich mit Google und unserer Datenschutzabteilung in Verbindung setzen](https://support.google.com/policies/troubleshooter/7575787?hl=de). Zusätzlich können Sie Ihre lokale Datenschutzaufsichtsbehörde kontaktieren, wenn Sie Bedenken bezüglich Ihrer Rechte gemäß dem örtlich geltenden Recht haben.

INFORMATIONEN ÜBER DIESE DATENSCHUTZERKLÄRUNG

Anwendungsbereich dieser Datenschutzerklärung

Diese Datenschutzerklärung gilt für alle Dienste, die von Google LLC und seinen [verbundenen Unternehmen](https://policies.google.com/privacy?hl=de#footnote-affiliates) angeboten werden, einschließlich YouTube, Android und Dienste, die auf Websites Dritter bereitgestellt werden, wie Werbedienste. Diese Datenschutzerklärung gilt nicht für Dienste, für die gesonderte Datenschutzrichtlinien gelten und die die vorliegende Datenschutzerklärung nicht beinhalten.

Diese Datenschutzerklärung gilt nicht für

* den Umgang mit Daten durch andere Unternehmen und Organisationen, die unsere Dienste bewerben,
* Dienste, die von anderen Unternehmen oder Personen angeboten werden, einschließlich Produkten oder Websites, die möglicherweise Google-Dienste beinhalten, sowie Dienste, die Ihnen in Suchergebnissen angezeigt werden oder die über einen Link in unseren Diensten erreicht werden können.

Änderungen an dieser Datenschutzerklärung

Wir ändern diese Datenschutzerklärung von Zeit zu Zeit. Wir werden Ihre Rechte im Rahmen dieser Datenschutzerklärung ohne Ihre ausdrückliche Zustimmung nicht einschränken. Wir geben immer das Veröffentlichungsdatum der letzten Änderungen an und bieten Ihnen Zugriff auf [archivierte Versionen](https://policies.google.com/privacy/archive?hl=de). Bei wesentlichen Änderungen weisen wir deutlicher auf diese hin. So werden Sie zum Beispiel bei bestimmten Diensten per E-Mail über eine Änderung der Datenschutzerklärung benachrichtigt.

WEITERE INFORMATIONEN ZUM DATENSCHUTZ

Google-Dienste

Die folgenden Datenschutzhinweise bieten zusätzliche Informationen zu manchen Google-Diensten:

* [Chrome und das Chrome-Betriebssystem](https://www.google.com/chrome/intl/de/privacy.html)
* [Payments](https://payments.google.com/legaldocument?family=0.privacynotice&hl=de)
* [Fiber](https://fiber.google.com/legal/privacy.html)
* [Google Fi](https://fi.google.com/about/tos/#project-fi-privacy-notice)
* [G Suite for Education](https://www.google.com/work/apps/terms/education_privacy.html)
* [Read Along](https://readalong.google/intl/de_CH/privacy)
* [YouTube Kids](https://kids.youtube.com/privacynotice)
* [Mit Family Link verwaltete Google-Konten für Kinder unter 13 Jahren (in einigen Ländern gilt ein anderes Mindestalter für Google-Konten)](https://families.google.com/familylink/privacy/child-policy/)
* [Erhebung von Sprach- und Audiodaten im Rahmen von Funktionen für Kinder in Google Assistant](https://assistant.google.com/privacy-notice-childrens-features/?hl=de)

Weitere hilfreiche Ressourcen

Die folgenden Links bieten hilfreiche Ressourcen, um weitere Informationen über unsere Praktiken und Datenschutzeinstellungen zu erhalten.

* [Ihr Google-Konto](https://myaccount.google.com/?hl=de) verfügt über zahlreiche Einstellungen, mit denen Sie Ihr Konto verwalten können.
* Der [Privatsphärecheck](https://myaccount.google.com/privacycheckup?utm_source=pp&utm_medium=Promo-in-product&utm_campaign=pp_body&hl=de) führt Sie durch die wichtigsten Datenschutzeinstellungen für Ihr Google-Konto.
* Im [Google Sicherheitscenter](https://www.google.com/intl/de/safetycenter/) erhalten Sie Informationen zu unseren integrierten Sicherheitsmaßnahmen und Datenschutzeinstellungen. Außerdem können Sie hier die Tools kennenlernen, mit denen Sie innerhalb Ihrer Familie Grundregeln für die Nutzung digitaler Onlinemedien aufstellen können.
* Der Abschnitt [Datenschutz & Nutzungsbedingungen](https://policies.google.com/?hl=de) bietet weitere Hintergrundinformationen zu dieser Datenschutzerklärung und zu unseren Nutzungsbedingungen.
* Unter [Technologien](https://policies.google.com/technologies?hl=de) finden Sie weitere Informationen zu folgenden Themen:
  + [So verwendet Google Cookies](https://policies.google.com/technologies/cookies?hl=de)
  + Die für [Werbung](https://policies.google.com/technologies/ads?hl=de) verwendeten Technologien
  + [Die Verwendung von Mustererkennung durch Google](https://policies.google.com/technologies/pattern-recognition?hl=de), um beispielsweise Gesichter in Fotos zu erkennen
  + [Wie wir Daten von Websites oder Apps verwenden, auf bzw. in denen unsere Dienste genutzt werden](https://policies.google.com/technologies/partner-sites?hl=de)

Amazon

Amazon Privacy Notice

**Last updated: January 1, 2020.** To see prior version, click [here](https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=16015091) .

We know that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This Privacy Notice describes how Amazon.com and its affiliates (collectively “Amazon”) collect and process your personal information through Amazon websites, devices, products, services, online and physical stores, and applications that reference this Privacy Notice (together “Amazon Services”). **By using Amazon Services, you are consenting to the practices described in this Privacy Notice.**

* [What Personal Information About Customers Does Amazon Collect?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_467C686A137847768F44B619694D3F7C)
* [For What Purposes Does Amazon Use Your Personal Information?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_7CE768C1281346DAAF87CE795E8B3610)
* [What About Cookies and Other Identifiers?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_0D132936501A4AE0A2F8D74426A8A2CA)
* [Does Amazon Share Your Personal Information?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_3DF674DAB5B7439FB2A9B4465BC3E0AC)
* [How Secure Is Information About Me?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_277A1D99140544EE9259ACA749AE3C3D)
* [What About Advertising?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_3F77537F901B4157B0CBD26834827652)
* [What Information Can I Access?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_002EF744608C4F9CAA7685BECC6C85FC)
* [What Choices Do I Have?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_697E8F46A0354B3B83E1A0D4C2FA52EE)
* [Are Children Allowed to Use Amazon Services?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_D17374D6EE5B4077946965351E11175C)
* [EU-US and Swiss-US Privacy Shield](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_A110DAC3F6BC4D5D9DDD59797104B1E5)
* [California Consumer Privacy Act](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_FE2374D302994717AB1A8CE585E7E8BE)
* [Conditions of Use, Notices, and Revisions](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_BA2E1D5A9B1F41CB86BCF0A40D9B8604)
* [Related Practices and Information](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_644071FEF22E48A2A160BAA332F95B27)
* [Examples of Information Collected](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01)

**What Personal Information About Customers Does Amazon Collect?**

We collect your personal information in order to provide and continually improve our products and services.

Here are the types of personal information we collect:

* **Information You Give Us:** We receive and store any information you provide in relation to Amazon Services. Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our Amazon Services.
* **Automatic Information:** We automatically collect and store certain types of information about your use of Amazon Services, including information about your interaction with content and services available through Amazon Services. Like many websites, we use "cookies" and other unique identifiers, and we obtain certain types of information when your web browser or device accesses Amazon Services and other content served by or on behalf of Amazon on other websites. Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01) to see examples of what we collect.
* **Information from Other Sources:** We might receive information about you from other sources, such as updated delivery and address information from our carriers, which we use to correct our records and deliver your next purchase more easily. Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01) to see additional examples of the information we receive.

**For What Purposes Does Amazon Use Your Personal Information?**

We use your personal information to operate, provide, develop, and improve the products and services that we offer our customers. These purposes include:

* **Purchase and delivery of products and services.** We use your personal information to take and handle orders, deliver products and services, process payments, and communicate with you about orders, products and services, and promotional offers.
* **Provide, troubleshoot, and improve Amazon Services.** We use your personal information to provide functionality, analyze performance, fix errors, and improve the usability and effectiveness of the Amazon Services.
* **Recommendations and personalization.** We use your personal information to recommend features, products, and services that might be of interest to you, identify your preferences, and personalize your experience with Amazon Services.
* **Provide voice, image and camera services.** When you use our voice, image and camera services, we use your voice input, images, videos, and other personal information to respond to your requests, provide the requested service to you, and improve our services. For more information about Alexa voice services , click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V) .
* **Comply with legal obligations.** In certain cases, we collect and use your personal information to comply with laws. For instance, we collect from sellers information regarding place of establishment and bank account information for identity verification and other purposes.
* **Communicate with you.** We use your personal information to communicate with you in relation to Amazon Services via different channels (e.g., by phone, e-mail, chat).
* **Advertising.** We use your personal information to display interest-based ads for features, products, and services that might be of interest to you. We do not use information that personally identifies you to display interest-based ads. To learn more, please read our [Interest-Based Ads](https://www.amazon.com/gp/help/customer/display.html?nodeId=202075050) notice .
* **Fraud Prevention and Credit Risks.** We use personal information to prevent and detect fraud and abuse in order to protect the security of our customers, Amazon, and others. We may also use scoring methods to assess and manage credit risks.

**What About Cookies and Other Identifiers?**

To enable our systems to recognize your browser or device and to provide and improve Amazon Services, we use cookies and other identifiers. For more information about cookies and how we use them, please read our [Cookies Notice](https://www.amazon.com/gp/help/customer/display.html/?nodeId=201890250) .

**Does Amazon Share Your Personal Information?**

Information about our customers is an important part of our business, and we are not in the business of selling our customers’ personal information to others. We share customers’ personal information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

* **Transactions involving Third Parties:** We make available to you services, products, applications, or skills provided by third parties for use on or through Amazon Services. For example, you can order products from third parties through our stores, download applications from third-party application providers from our App Store, and enable third-party skills through our Alexa services. We also offer services or sell product lines jointly with third-party businesses, such as co-branded credit cards. You can tell when a third party is involved in your transactions, and we share customers’ personal information related to those transactions with that third party.
* **Third-Party Service Providers:** We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders for products or services, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing payments, transmitting content, scoring, assessing and managing credit risk, and providing customer service. These third-party service providers have access to personal information needed to perform their functions, but may not use it for other purposes.
* **Business Transfers:**As we continue to develop our business, we might sell or buy other businesses or services. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc. or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.
* **Protection of Amazon and Others:** We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our [Conditions of Use](https://www.amazon.com/gp/help/customer/display.html?nodeId=201909000) and other agreements; or protect the rights, property, or safety of Amazon, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction.

Other than as set out above, you will receive notice when personal information about you might be shared with third parties, and you will have an opportunity to choose not to share the information.

**How Secure Is Information About Me?**

We design our systems with your security and privacy in mind.

* We work to protect the security of your personal information during transmission by using encryption protocols and software.
* We follow the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card data.
* We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal customer information. Our security procedures mean that we may occasionally request proof of identity before we disclose personal information to you.
* Our devices offer security features to protect them against unauthorized access and loss of data. You can control these features and configure them based on your needs. Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=200127470) for more information on how to manage the security settings of your device.
* It is important for you to protect against unauthorized access to your password and to your computers, devices, and applications. Be sure to sign off when finished using a shared computer. Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=201293120) for more information on how to sign off.

**What About Advertising?**

* **Third-Party Advertisers and Links to Other Websites:** Amazon Services may include third-party advertising and links to other websites and apps. Third-party advertising partners may collect information about you when you interact with their content, advertising, and services. For more information about third-party advertising at Amazon, including interest-based ads, please read our [Interest-Based Ads](https://www.amazon.com/gp/help/customer/display.html?nodeId=202075050) policy . To adjust your advertising preferences, please go to the [Advertising Preferences](https://www.amazon.com/adprefs) page .
* **Use of Third-Party Advertising Services:** We provide ad companies with information that allows them to serve you with more useful and relevant Amazon ads and to measure their effectiveness. We never share your name or other information that directly identifies you when we do this. Instead, we use an advertising identifier like a cookie or other device identifier. For example, if you have already downloaded one of our apps, we will share your advertising identifier and data about that event so that you will not be served an ad to download the app again. Some ad companies also use this information to serve you relevant ads from other advertisers. You can learn more about how to opt-out of interest-based advertising by going to the [Advertising Preferences](https://www.amazon.com/adprefs) page .

**What Information Can I Access?**

You can access your information, including your name, address, payment options, profile information, Prime membership, household settings, and purchase history in the "Your Account" section of the website. Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01) for a list of examples that you can access.

**What Choices Do I Have?**

If you have any questions as to how we collect and use your personal information, please contact our [Customer Service](https://www.amazon.com/gp/help/contact-us) . Many of our Amazon Services also include settings that provide you with options as to how your information is being used.

* As described above, you can choose not to provide certain information, but then you might not be able to take advantage of many of the Amazon Services.
* You can add or update certain information on pages such as those referenced in [What Information Can I Access?](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_002EF744608C4F9CAA7685BECC6C85FC). When you update information, we usually keep a copy of the prior version for our records.
* If you do not want to receive e-mail or other communications from us, please adjust your [Customer Communication Preferences](https://www.amazon.com/gp/cpc/homepage?ref=gss_to_cpc) . If you don’t want to receive in-app notifications from us, please adjust your notification settings in the app or device.
* If you do not want to see interest-based ads, please adjust your [Advertising Preferences](https://www.amazon.com/adprefs) .
* The Help feature on most browsers and devices will tell you how to prevent your browser or device from accepting new cookies or other identifiers, how to have the browser notify you when you receive a new cookie, or how to block cookies altogether. Because cookies and identifiers allow you to take advantage of some essential features of Amazon Services, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Services that require you to Sign in. For more information about cookies and other identifiers, see our [Cookies Notice](https://www.amazon.com/gp/help/customer/display.html/?nodeId=201890250) .
* If you want to browse our websites without linking the browsing history to your account, you may do so by logging out of your account [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=201293120) and blocking cookies on your browser.
* You will also be able to opt out of certain other types of data usage by updating your settings on the applicable Amazon website (e.g., in "Manage Your Content and Devices"), device, or application. For more information click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=GQFYXZHZB2H629WN) . Most non-Amazon devices also provide users with the ability to change device permissions (e.g., disable/access location services, contacts). For most devices, these controls are located in the device's settings menu. If you have questions about how to change your device permissions on devices manufactured by third parties, we recommend you contact your mobile service carrier or your device manufacturer.
* If you are a seller, you can add or update certain information in [Seller Central](https://sellercentral.amazon.com/) , update your account information by accessing your [Seller Account Information](https://sellercentral.amazon.com/hz/sc/account-information) , and adjust your e-mail or other communications you receive from us by updating your [Notification Preferences](https://sellercentral.amazon.com/notifications/preferences/ref=xx_notifpref_dnav_xx) .
* If you are an author, you can add or update the information you have provided in the [Author Portal](https://authorcentral.amazon.com/gp/help?topicID=200649520) and [Author Central](https://authorcentral.amazon.com/) by accessing your accounts in the Author Portal and Author Central, respectively.

In addition, to the extent required by applicable law, you may have the right to request access to or delete your personal data. If you wish to do any of these things, please contact [Customer Service](https://www.amazon.com/gp/help/contact-us) . Depending on your data choices, certain services may be limited or unavailable.

**Are Children Allowed to Use Amazon Services?**

Amazon does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon Services only with the involvement of a parent or guardian. We do not knowingly collect personal information from children under the age of 13 without the consent of the child's parent or guardian. For more information, please see our [Children's Privacy Disclosure](https://www.amazon.com/gp/help/customer/display.html?nodeId=202185560) .

**EU-US and Swiss-US Privacy Shield**

Amazon.com, Inc. participates in the EU-US and Swiss-US Privacy Shield frameworks. Click [here](https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=202135380) to learn more.

**California Consumer Privacy Act**

Click [here](https://www.amazon.com/gp/help/customer/display.html?nodeId=GC5HB5DVMU5Y8CJ2) to read additional disclosures required under the California Consumer Privacy Act.

**Conditions of Use, Notices, and Revisions**

If you choose to use Amazon Services, your use and any dispute over privacy is subject to this Notice and our [Conditions of Use](https://www.amazon.com/gp/help/customer/display.html?nodeId=201909000) , including limitations on damages, resolution of disputes, and application of the law of the state of Washington. If you have any concern about privacy at Amazon, please contact us with a thorough description, and we will try to resolve it. Our business changes constantly, and our Privacy Notice will change also. You should check our websites frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

**Related Practices and Information**

* [Conditions of Use](https://www.amazon.com/gp/help/customer/display.html?nodeId=201909000)
* [Seller Program Policies](https://www.amazon.com/gp/help/customer/display.html/ref=hp_468496_crules?nodeId=537776)
* [Help Department](https://www.amazon.com/gp/browse.html/ref=hp_468496_help?node=508510)
* [Most Recent Purchases](https://www.amazon.com/your-orders)
* [Your Profile and Community Guidelines](https://www.amazon.com/gp/browse.html/ref=hp_468496_yourprofile?node=14279631)

**Examples of Information Collected**

**Information You Give Us When You Use Amazon Services**

You provide information to us when you:

* search or shop for products or services in our stores;
* add or remove an item from your cart, or place an order through or use Amazon Services;
* download, stream, view, or use content on a device or through a service or application on a device;
* provide information in [Your Account](https://www.amazon.com/gp/css/homepage.html/ref=hp_468496_youraccount) (and you might have more than one if you have used more than one e-mail address or mobile number when shopping with us) or [Your Profile](https://www.amazon.com/gp/pdp/profile) ;
* talk to or otherwise interact with our Alexa Voice service;
* upload your contacts;
* configure your settings on, provide data access permissions for, or interact with an Amazon device or service;
* provide information in your [Seller Account](https://sellercentral.amazon.com/) , [Kindle Direct Publishing](https://kdp.amazon.com/) account , [Developer](https://developer.amazon.com/) account , or any other account we make available that allows you to develop or offer software, goods, or services to Amazon customers;
* offer your products or services on or through Amazon Services;
* communicate with us by phone, e-mail, or otherwise;
* complete a questionnaire, a support ticket, or a contest entry form;
* upload or stream images, videos or other files to Prime Photos, Amazon Drive, or other Amazon Services;
* use our services such as Prime Video;
* compile Playlists, Watchlists, [Wish Lists](https://www.amazon.com/gp/registry/wishlist-homepage.html/ref=hp_468496_wishlist2) or other gift registries;
* participate in Discussion Boards or other community features;
* provide and rate [Reviews](https://www.amazon.com/gp/help/customer/display.html/?nodeId=200791000) ;
* specify a Special Occasion Reminder; or
* employ [Product Availability Alerts](https://www.amazon.com/gp/help/customer/display.html?nodeId=569162) , such as Available to Order Notifications.

**As a result of those actions, you might supply us with such information as:**

* identifying information such as your name, address, and phone numbers;
* payment information;
* your age;
* your location information;
* your IP address;
* people, addresses and phone numbers listed in your Addresses;
* e-mail addresses of your friends and other people;
* content of reviews and e-mails to us;
* personal description and photograph in [Your Profile](https://www.amazon.com/gp/pdp/profile) ;
* voice recordings when you speak to Alexa;
* images and videos collected or stored in connection with Amazon Services;
* information and documents regarding identity, including Social Security and driver's license numbers;
* corporate and financial information;
* credit history information; and
* device log files and configurations, including Wi-Fi credentials, if you choose to automatically synchronize them with your other Amazon devices.

**Automatic Information**

Examples of the information we collect and analyze include:

* the internet protocol (IP) address used to connect your computer to the internet;
* login, e-mail address, and password;
* the location of your device or computer;
* content interaction information, such as content downloads, streams, and playback details, including duration and number of simultaneous streams and downloads, and network details for streaming and download quality, including information about your internet service provider;
* device metrics such as when a device is in use, application usage, connectivity data, and any errors or event failures;
* Amazon Services metrics (e.g., the occurrences of technical errors, your interactions with service features and content, your settings preferences and backup information, location of your device running an application, information about uploaded images and files such as the file name, dates, times and location of your images);
* version and time zone settings;
* purchase and content use history, which we sometimes aggregate with similar information from other customers to create features like [Top Sellers](https://www.amazon.com/gp/bestsellers) ;
* the full Uniform Resource Locator (URL) clickstream to, through, and from our websites, including date and time; products and content you viewed or searched for; page response times, download errors, length of visits to certain pages, and page interaction information (such as scrolling, clicks, and mouse-overs);
* phone numbers used to call our customer service number; and
* images or videos when you shop in our stores, or stores using Amazon Services.

We may also use device identifiers, cookies, and other technologies on devices, applications, and our web pages to collect browsing, usage, or other technical information.

**Information from Other Sources**

Examples of information we receive from other sources include:

* updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily;
* account information, purchase or redemption information, and page-view information from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising, or other services;
* information about your interactions with products and services offered by our subsidiaries;
* search results and links, including paid listings (such as Sponsored Links);
* information about internet-connected devices and services linked with Alexa; and
* credit history information from credit bureaus, which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers.

**Information You Can Access**

Examples of information you can access through Amazon Services include:

* status of recent orders (including subscriptions);
* your complete order history;
* personally identifiable information (including name, e-mail, password, and address book);
* payment settings (including payment card information, promotional certificate and gift card balances, and 1-Click settings);
* e-mail notification settings (including Product Availability Alerts, Delivers, Special Occasion Reminders and newsletters);
* recommendations and the products you recently viewed that are the basis for recommendations (including Recommended for You and Improve Your Recommendations);
* shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries);
* your content, devices, services, and related settings, and communications and personalized advertising preferences;
* content that you recently viewed;
* voice recordings associated with your account;
* Your Profile (including your product Reviews, Recommendations, Reminders and personal profile);
* If you are a seller, you can access your account and other information, and adjust your communications preferences, by updating your account in [Seller Central](https://sellercentral.amazon.com/) .
* If you are an author, you can access your account and other information, and update your accounts, on the [Kindle Direct Publishing (KDP)](https://kdp.amazon.com/) or [Author Central](https://authorcentral.amazon.com/) website, as applicable.
* If you are a developer participating in our Developer Services Program, you can access your account and other information, and adjust your communications preferences, by updating your accounts in the [Developer Services Portal](https://developer.amazon.com/) .

Pinterest

**We collect information in a few different ways**

* **1. When you give it to us or give us permission to obtain it**

When you sign up for or use Pinterest you voluntarily share certain information including your name, email address, phone number, photos, Pins, comments, and any other information you give us. You can also choose to share your precise location using your device settings or through photos. We will still use your IP address, which is used to approximate your location, even if you don't choose to share your precise location. You will also have the option to share other information about yourself such as your gender, age and preferred language.  
      
If you [connect your Facebook, Google(opens in a new window)](https://help.pinterest.com/article/link-your-social-media) or other third-party accounts to Pinterest, we use information from those accounts (such as your friends or contacts) to improve your Pinterest experience. This is dependent on the privacy policies or settings for those accounts.

**2. We also get technical information when you use Pinterest**

When you use a website, mobile application or other internet service, certain internet and electronic network activity information gets created and logged automatically. This is also true when you use Pinterest. Here are some of the types of information we collect:

* + **Log data.** When you use Pinterest, our servers record information (“log data”), including information that your browser automatically sends whenever you visit a website, or that your mobile app automatically sends when you’re using it. This log data includes your Internet Protocol address (which we use to infer your approximate location), the address of and activity on websites you visit that incorporate Pinterest features (like the “Save” button—more details below), searches, browser type and settings, the date and time of your request, how you used Pinterest, cookie data and device data. You can [learn more about the log data we collect here](https://policy.pinterest.com/technical-information-we-collect-when-you-use-our-service).
  + **Cookie data.** We also use “cookies” (small text files sent by your computer each time you visit our website, unique to your Pinterest account or your browser) or similar technologies to get log data. When we use cookies or other similar technologies, we use session cookies (that last until you close your browser) or persistent cookies (that last until you or your browser delete them). For example, we use cookies to store your language preferences or other settings so you don‘t have to set them up every time you visit Pinterest. Some of the cookies we use are associated with your Pinterest account (including information about you, such as the email address you gave us) and other cookies are not. For more detailed information about how we use cookies, please review our [Cookie Policy(opens in a new window)](https://policy.pinterest.com/cookies).
  + **Device information.** In addition to log data, we collect information about the device you’re using Pinterest on, including the type of device, operating system, settings, unique device identifiers and crash data that helps us understand when something breaks.
  + **Clickstream data and inferences.** When you’re on Pinterest, we use your activity—such as which Pins you click on, boards you create, and any text that you add in a comment or description—along with information you provided when you first signed up and information from our partners and advertisers to make inferences about you and your preferences. For example, if you create a board about travel, we may infer you are a travel enthusiast. We may also infer information about your education or professional experience based on your activity when you [link your account to accounts you have with third parties like Facebook or Google](https://help.pinterest.com/article/link-your-social-media).

**3. Our partners and advertisers share information with us**

We also get information about you and your activity outside Pinterest from our affiliates, advertisers, partners and other third parties we work with. For example:

* + Some websites or apps use Pinterest features such as our “Save” button, or you may install our “Save” button for your browser. If so, we collect log data from those sites or apps. [You can learn more about these features at our Help Center.](https://help.pinterest.com/article/save-pins-with-the-pinterest-browser-button)
  + Online advertisers or third parties share information with us to measure, report on or improve the performance of ads on Pinterest, or to figure out what kinds of ads to show you on or off of Pinterest. This includes information about your visits to an advertiser's site or purchases you made from them, or information about your interests from a third-party service, which we might use to help show you ads. [Learn more about the types of information advertisers or other third parties share with us](https://help.pinterest.com/article/personalized-ads-on-pinterest).

**What we do with the info we collect**

* **We’re committed to showing you content that’s relevant, interesting and personal to you. To do that, we use your information to provide and improve your experience, including:**
  + Identify you when you use Pinterest.
  + Recommend Pins, boards, topics or categories you might like based on your activity on Pinterest. For example, if we see you’re into cooking, we may suggest food-related Pins, boards or people that we think you might like, or show you food-related ads.
  + Respond to your questions or comments.

We have a legitimate interest for using your info in these ways. It's fundamental to what we do at Pinterest and necessary in order to make Pinterest and its features relevant and personalized to you.

We also have a legitimate interest in making Pinterest safe and improving our product features so you keep finding the inspiration you want. We all benefit when we use your information to:

* + Suggest other people who have similar interests. For example, if you follow interior design boards, we may suggest interior designers that you might like.
  + Help your friends and contacts find you on Pinterest, if you agree to this in your settings. For example, if you sign up using a Facebook account, we can help your Facebook friends find you on Pinterest when they first sign up for Pinterest. Or people can search for your account on Pinterest using your email.
  + Work with law enforcement and keep Pinterest safe. We may get requests for account information from law enforcement authorities like the police or courts. To find out more about how we respond to law enforcement requests, please see our [Law Enforcement Guidelines](https://help.pinterest.com/article/law-enforcement-guidelines).
  + Review your messages on Pinterest to detect activity that poses a risk to the safety of you, our community and/or members of the public.
  + Conduct analytics and research on who is using Pinterest and what they are doing. For example, by logging how often people use two different versions of a feature on Pinterest, we can understand which version is better.
  + Improve Pinterest and offer new features.
  + Advertise Pinterest products and services to you on other sites. You can choose for us not to share your information with other sites to personalize those ads as described in the “[Choices you have about your information](https://policy.pinterest.com/privacy-policy#section-choices-you-have-about-your-info)” section below.
  + Send you updates (such as when certain activity, like saves or comments, happens on Pinterest) and news by email or push notification, depending on your settings. For example, we send weekly updates that include Pins you may like. You can decide to [stop getting these notifications](https://help.pinterest.com/article/edit-notification-settings) by updating your [settings](https://www.pinterest.com/settings/).

We have a legitimate interest in delivering ads that are relevant, interesting and personal to you in order to generate revenue. To further these interests we use the information we collect to:

* + Decide which ads to show you. For example, if you show an interest in camping tents on Pinterest, we may show you ads for other outdoor products. We customize the ad content we show you by identifying your interests based on your onsite and offsite activities, as well as by using information we receive from ad partners or other third parties. Where we use cookies to identify your offsite interests, we’ll get your consent where we need to. Where ad partners or other third parties share information with us about you, we rely on the consent they already obtained.
  + Tell our ad partners how their Pinterest ads are doing, and how to make them better. Some of this information is aggregated. For example, we would report to an advertiser that a certain percentage of people who viewed a Promoted Pin went on to visit that advertiser's site. In other instances, this information isn’t aggregated. For example, we would let an advertiser know that a particular Promoted Pin has been saved by certain people. To find out more about reporting on ads please [visit the Help Center](https://help.pinterest.com/articles/ads-performance-reporting-pinterest).

We have a legitimate interest in using information we collect to customize your Pinterest experience based on your offsite behavior. For example, if you visit websites that sell electric guitars, we may suggest guitar Pins to you. When we identify your interests based on your offsite behavior with cookies, we will obtain any consent that we may need. To find out more about how we use cookies, please see our [Cookie Policy](https://policy.pinterest.com/cookies).

In addition to the specific circumstances above, we’ll only use your information with your consent in order to:

* + Allow searching with photos. For example, if you take a photo of a pair of shoes or a piece of furniture you like, you can ask us to show you similar items. You can opt in to this in your device operating system settings.
  + Send you marketing materials by email, text, push notification or phone call depending on your account or operating system settings. Each time we send you marketing materials, we give you the option to unsubscribe.
  + Identify your precise location and customize the content we show you. For example, if we know that you’re near a retailer we may show you that retailer’s Pins that may be of interest to you. You can opt in to this in your device operating system settings.
  + Tell our ad partners how their ads are doing using the Pinterest Tag. The Pinterest Tag (a piece of code an advertiser puts on their site) delivers insights to us and our ad partners about actions that a person takes on their website after viewing an ad on Pinterest. [To learn more about the Pinterest Tag, please visit the Help Center](https://help.pinterest.com/article/personalization-and-data).

We’ll also rely on your consent where we use cookies to:

* + Identify you across different browser sessions. This means if you log into Pinterest from your phone (or any device), we'll remember that you're you and then you won't need to enter your login details each time you visit Pinterest.
  + Show you ads you might be interested in. We use cookies to identify your interests based on your offsite activity. We do this for people currently using Pinterest and for new folks, and it helps us customize how you get started on Pinterest.

To find out more about how we use cookies, and your choices about how we use them, please see our [Cookie Policy](https://policy.pinterest.com/cookie-policy-preview).

**Transferring your information**

* Pinterest is a worldwide service. By using our products or services, you authorize us to transfer and store your information outside your home country, including in the United States, for the purposes described in this policy. The privacy protections and the rights of authorities to access your personal information in such countries may not be equivalent to those of your home country.

See the [section for EEA Residents](https://policy.pinterest.com/privacy-policy#section-residents-of-the-eea) to learn more about data transfers to and from that region.

**Choices you have about your info**

* Our goal is to give you simple and meaningful choices regarding your information. If you have a Pinterest account, many of these controls are built directly into Pinterest or your settings. For example, you can:
  + [Edit information in your profile](https://help.pinterest.com/article/edit-your-profile) at any time, decide whether your profile is available to search engines, or choose whether others can find your Pinterest account using your email address.
  + [Link or unlink your Pinterest account](https://help.pinterest.com/article/link-your-social-media) from other services (like Facebook, Google or Twitter). For some services (like Facebook), you can also decide whether or not to publish your Pinterest activity to that service.
  + [Edit secret board settings](https://help.pinterest.com/article/secret-boards). Secret boards are visible to you and other collaborators in the board, and any collaborator may choose to make the board available to anyone else. For example, another collaborator can invite someone else to the board, make the board available to an app they use to view Pinterest, or even just take an image from the board and email it to their friends.
  + [Choose whether Pinterest will be customized for you using information from other websites or apps](https://help.pinterest.com/article/edit-personalization-settings). If you have a Pinterest account and want to control how your offsite data is used to tailor your experience, you can visit [your settings](https://help.pinterest.com/article/edit-personalization-settings) and update your “Personalization” preferences.
  + Choose whether Pinterest ads delivered to you on other platforms, sites or apps are customized using information about your account activities. You can control this by visiting [your settings](https://www.pinterest.com/settings/) and updating your “Personalization” preferences.
  + Choose whether Pinterest shares information about your activity on Pinterest for ads performance reporting. You can control this by visiting [your settings](https://www.pinterest.com/settings/privacy) and updating your “Personalization” preferences.
  + [Close your account at any time](https://help.pinterest.com/article/deactivate-or-close-your-account). When you close your account, we’ll deactivate it, remove your Pins and boards from Pinterest and delete your account data. Please note that there may be legal reasons for us to keep your data, such as if we receive a law enforcement request asking us to preserve data. We may also retain certain information in our backup systems for a limited period of time, or as required by law.

We also support settings such as Limit Ad Tracking in iOS, Ads Personalization in Android devices as well as [Do Not Track](https://help.pinterest.com/article/do-not-track) in browsers. [Learn more about how Do Not Track affects our collection and use of data collected off of Pinterest](https://help.pinterest.com/article/do-not-track).

You also have choices available to you through the device or software you use to access Pinterest. For example:

* + The browser you use lets you control cookies or other types of local data storage.
  + Your mobile device lets you choose how and whether your precise location, photos, contacts and other data is shared with us.

To learn more about these choices, please see the information provided by your device or software provider.

**How and when we share information**

* Anyone can see the public boards and Pins you create and profile information you give us. We also make this public information available through what are called APIs (basically a technical way to share information quickly). For example, a partner can study what their most popular Pins are or how their Pins are being shared on Pinterest by using a Pinterest API. We also share your information with:
  + Other services, at your direction, to enable you to sign up for or log in to Pinterest, or when you decide to [link your Pinterest account](https://help.pinterest.com/article/link-your-social-media) to those services, like Facebook or Google, or when you publish your content on Pinterest to them. For example, if you choose to publish your Pins to Facebook or Twitter, then information about that content will be shared with Facebook or Twitter.
  + Services we use to market Pinterest to you on sites and apps other than Pinterest, such as Facebook Ads, Google Marketing Platform, Microsoft Advertising, LinkedIn Advertising, The Trade Desk and others from time to time. You can opt-out of sharing with such advertising services in your settings.
  + Online advertisers and third-party companies that we or they use to audit or improve the delivery and performance of ads or content on websites and apps (for example, through Google Analytics). This includes us sharing the Pins or ads you were shown on Pinterest and whether or how you engaged with those Pins or ads, or other information about your activity on Pinterest. [Learn more about how we share information with online advertisers](https://help.pinterest.com/article/personalized-ads-on-pinterest). [To learn more about third-party companies that analyze ad performance, please visit our Help Center](https://help.pinterest.com/article/personalized-ads-on-pinterest).
  + Third-party companies, service providers or individuals that we employ to process information on our behalf based on our instructions and for the purposes described in this Privacy Policy. For example, we share data with security consultants to help us get better at identifying spam. Some information we acquire may be collected by third-party providers on our behalf.
  + Law enforcement agencies or government agencies. We only share information if we believe that disclosure is reasonably necessary to comply with a law, regulation or legal request; to protect the safety, rights, or property of the public, any person, or Pinterest; or to detect, prevent, or otherwise address fraud, security or technical issues.
  + Our wholly-owned subsidiaries and affiliates. If we were to engage in a merger, acquisition, bankruptcy, dissolution, reorganization, or similar transaction or proceeding that involves the transfer of the information described in this Policy, we would share your information with a party involved in such a process (for example, a potential purchaser).

**How long we keep your information**

* We keep your information only so long as we need it to provide Pinterest to you and fulfill the purposes described in this policy. This is also the case for anyone that we share your information with and who carries out services on our behalf. When we no longer need to use your information and there is no need for us to keep it to comply with our legal or regulatory obligations, we’ll either remove it from our systems or depersonalize it so that we can't identify you.

**Our policy on children’s information**

* Children under 13 are not allowed to use Pinterest. If you are based in the EEA you may only use Pinterest if you are over the age at which you can provide consent to data processing under the laws of your country.

**Your options**

* You have options in relation to the information that we have about you. To exercise these options, please visit your [account settings](https://www.pinterest.com/settings/privacy) and, if you still need help, our [Help Center](https://help.pinterest.com/).
  + Request access to the information we collect and hold about you. We'll usually share this with you within 30 days of you [asking us for it through our Help Center](https://help.pinterest.com/contact?current_page=about_you_page&personal_data=personal_data_view).
  + Have your information corrected or deleted. You can update your information in your profile or delete your data by [closing your account](https://help.pinterest.com/article/deactivate-or-close-your-account).
  + Object to us processing your information. You can ask us to stop using your information, including when we use your information to send you marketing emails or push notifications. If you opt out of receiving marketing messages from us, we may still send you updates about your account, such as when someone comments on one of your Pins.
  + Have the information you provided to us sent to another organization, where we hold this information with your consent or for the performance of a contract with you, and, where it's technically feasible for us to do so.
  + Request more details about the information we collect and how and why we use and share it.

We will not discriminate against you if you choose to exercise your options related to your personal information. We work to be clear with you about your options and the consequences of exercising certain options. If you have questions, please [contact us](https://help.pinterest.com/contact).

**Residents of the EEA**

* If you have any questions about our data processing activities, the data controller you should contact is Pinterest Europe Ltd., an Irish company with its registered office at Palmerston House, 2nd Floor, Fenian Street, Dublin 2, Ireland. You can also contact our [Data Protection Officer](https://help.pinterest.com/data-protection-officer-contact-form).

If you think that we haven't complied with data protection laws, you have a right to lodge a complaint with the Data Protection Commission in Ireland or with your local supervisory authority.

Because Pinterest is a worldwide service, we may transfer the personal data of EEA residents to a country outside the EEA. Where we transfer information from the EEA to a country that doesn't provide an adequate level of protection, we’ll only do so under appropriate safeguards to protect your information, like standard contractual clauses.

**California residents**

* The California Consumer Privacy Act (CCPA) requires us to disclose categories of Personal Information we collect and how we use it, the categories of sources from whom we collect Personal Information, and the third parties with whom we share it, which we have explained above.

In the preceding twelve months, we have collected Personal Information from you, your devices, our partners, third parties, and from categories of sources otherwise described in the [“We collect information in a few different ways”](https://policy.pinterest.com/privacy-policy#section-we-collect-information-in-a-few-different-ways) section of this Privacy Policy.

We are also required to communicate information about rights California residents have under California law. You may exercise the following rights:

* + Right to Know and Access. You may submit a verifiable request for information regarding the: (1) categories of Personal Information we collect, use, or share; (2) purposes for which categories of Personal Information are collected or used by us; (3) categories of sources from which we collect Personal Information; and (4) specific pieces of Personal Information we have collected about you.
  + Right to Equal Service. We will not discriminate against you if you exercise your privacy rights.
  + Right to Delete. You may submit a verifiable request to close your account and we will delete Personal Information about you that we have collected.

In order to verify your identity when you make a request, you will be required to log in to your password-protected account or respond to an email verification request.

We do not sell the Personal Information of our users.

For more information about these rights, please see “Choices you have about your info” above, and to exercise them, please [visit our Help Center](https://help.pinterest.com/contact?current_page=about_you_page&personal_data=personal_data_view) or contact us at [privacy-support@pinterest.com](mailto:privacy-support@pinterest.com).

In addition to exercising these rights yourself, you may also designate an authorized agent to make these requests on your behalf. In order to do this, we will ask you to verify the request directly via email or through your password-protected account.

We collect the following categories of Personal Information and in the past 12 months, we have disclosed these categories of Personal Information for a business purpose to affiliates, service providers and third parties, as described in the [How and when we share information](https://policy.pinterest.com/privacy-policy#section-how-and-when-we-share-information) section of this Privacy Policy:

* + Identifiers, such as your name, username, email address, phone number, unique device identifiers, and your IP address
  + Personal characteristics protected by law, such as your gender and age
  + Commercial information, such as purchases made, and payment information
  + Internet or electronic network activity information, such as information about your device and your use of our Services
  + Geo-location data, when shared through your device settings or photos
  + Electronic, visual, or similar information, such as your profile picture or photos
  + Professional or employment information, when you link your account to other accounts
  + Inferences we draw or derive about users, such as your interests or preferences
  + Other information you provide, such as your bio, Pins, and comments

We use and disclose this information for the business purposes described in the [What we do with the info we collect](https://policy.pinterest.com/privacy-policy#section-what-we-do-with-the-info-we-collect) section in this Privacy Policy, including to: provide our Service, communicate with you to provide updates or respond to your comments and questions, audit our Service, detect security incidents and prevent fraud, debug and repair errors, maintain your account, provide customer service, process or fulfill orders, conduct research and development and other activities to improve our Service, show advertising, market our Services, and understand how users interact with our Services.

**How we make changes to this policy**

* We may change this policy from time to time and if we do, we’ll post any changes on this page. If you continue to use Pinterest after those changes are in effect, you agree to the new policy. If the changes are significant, we may provide a more prominent notice or get your consent, as required by law.

**Contact us**

* The best way to get in touch with us or to exercise your options described above is through the [Help Center](https://help.pinterest.com/contact). If you live in the United States, Pinterest, Inc. is responsible for your information. You can contact Pinterest Inc. at 651 Brannan Street, San Francisco, CA 94107, USA.

Zalando

**Für welche Angebote und Dienstleistungen gilt diese Datenverarbeitungserklärung:** Art und Methoden der von Zalando durchgeführten Datenverarbeitung sind für die meisten unserer Angebote ähnlich. Diese Datenverarbeitungserklärung gilt daher für alle Dienstleistungen und Dienstleistungen, die wir unseren Kunden in Europa anbieten. Dies gilt unabhängig von der Plattform, auf der wir den Service anbieten: Website, App, in Verkaufsstellen, telefonisch, bei Veranstaltungen oder über soziale Netzwerke. Der Einfachheit halber verwenden wir in diesen "normalen Fällen" den Begriff "Dienstleistungen".

Es gibt jedoch auch Dienste, für die wir Ihre Daten auf andere Weise oder für andere Zwecke verarbeiten. Dies kann von der Art der Dienstleistung oder von länderspezifischen Anforderungen abhängen. Wenn wir uns auf diese Fälle beziehen (daher "Ausnahmen vom Normalfall"), sprechen wir von "dienstspezifisch" oder "länderspezifisch".

Schließlich muss berücksichtigt werden, dass Zalando kein einziges Unternehmen ist. Zalando ist eine Gruppe und besteht daher aus zahlreichen Unternehmen. Nicht jeder von ihnen bietet alle Dienstleistungen an oder führt die gesamte Datenverarbeitung durch. Der Einfachheit halber sind nachfolgend nur die Unternehmen der Zalando-Gruppe aufgeführt, die tatsächlich mit der Verarbeitung Ihrer Daten zu tun haben. Wenn wir im Folgenden von "Zalando" oder "wir" sprechen, meinen wir die Unternehmen, die jeweils für die Zalando-Gruppe verantwortlich sind.

Dies bezieht sich insbesondere auf die folgenden Zalando-Unternehmen

**Was lernen Sie mit dieser Datenverarbeitungserklärung:**

* Welche Daten werden von Zalando gespeichert?
* Was machen wir mit diesen Daten und wofür werden sie benötigt?
* Welche Datenschutzrechte und welche Möglichkeiten haben Sie?
* Welche Technologien und Daten wir verwenden, um unsere Dienste und Inhalte zu personalisieren und anzupassen, verwenden wir, um Ihnen ein sicheres, einfaches, nahtloses und individuelles Einkaufserlebnis zu bieten.
* Welche Technologien und welche Daten verwenden wir für Werbung, einschließlich Tracking-Technologien.

**1. Welche Daten werden von Zalando verarbeitet?**

Zalando bietet verschiedene Dienstleistungen an, die Sie auf unterschiedliche Weise genießen können. Je nachdem, ob Sie uns online, telefonisch, persönlich oder auf andere Weise kontaktieren, kommen unterschiedliche Daten aus unterschiedlichen Quellen ins Spiel. Ein Großteil der von uns verarbeiteten Daten wird uns von Ihnen mitgeteilt, während Sie unsere Dienste nutzen, beispielsweise wenn Sie uns kontaktieren und sich unter Angabe Ihres Namens, Ihrer E-Mail-Adresse oder Ihrer Adresse registrieren. Wir erhalten jedoch auch technische Daten zu den Geräten und zum Zugriff, die bei der Interaktion mit unseren Diensten automatisch erfasst werden. Diese können sich auf den von Ihnen verwendeten Gerätetyp beziehen. Weitere Daten erheben wir auf Basis von Analysen, die wir durchführen (z. B. im Rahmen von Marktforschung oder Kundenbewertung). Möglicherweise erhalten wir auch Daten von Dritten über Sie, z. B. Geschäftsinformationsdienste oder Zahlungsdienstleister.

Wenn wir von "Daten" sprechen, beziehen wir uns auf personenbezogene Daten. Dies sind Informationen, anhand derer wir Sie sofort identifizieren oder mit anderen Informationen kombinieren können. Beispiele: Ihr Name, Telefonnummer, Kundennummer, Bestellnummer oder Ihre E-Mail-Adresse. Alle Informationen, die es uns nicht ermöglichen, Sie zu identifizieren (auch nicht durch Kombination mit anderen Informationen), gelten als nicht personenbezogene Daten. Nicht personenbezogene Daten werden auch als anonymisierte Daten bezeichnet. Wenn wir personenbezogene Daten mit anonymisierten Daten kombinieren, gelten alle Daten in dieser Datenreihe als personenbezogene Daten. Wenn wir die personenbezogenen Daten einer Reihe von Daten oder Informationen über Sie löschen, gelten die verbleibenden Daten dieser Datenreihe nicht mehr als personenbezogene Daten. Dieser Vorgang wird als Anonymisierung bezeichnet. Grundsätzlich gilt dies: Wenn wir Sie um die Angabe bestimmter personenbezogener Daten bitten, können Sie dies natürlich ablehnen. Sie entscheiden, welche Informationen Sie uns geben möchten. Es ist jedoch möglich, dass wir Ihnen die gewünschten Dienstleistungen nicht oder nicht optimal anbieten können. Beispielsweise ist es nicht möglich, Pakete ohne Angabe einer Lieferadresse zuzustellen.

**1.1. Profildaten**

Profildaten sind persönliche und demografische Daten über Sie (sogenannte Basisdaten) und Ihre individuellen Interessen, die Sie uns bei der Registrierung Ihres Kundenkontos mitteilen. Zu den Profildaten gehören zum Beispiel:

* Ihr Vor- und Nachname;
* Ihre Kontaktdaten;
* Ihre Vorlieben, zum Beispiel in Bezug auf Marken, Produktgenres oder Stile;
* Demografie wie Geschlecht, Alter und Wohnort.

Die obligatorischen Daten sind normalerweise Ihr Name, Ihre Adresse und E-Mail-Adresse sowie das von Ihnen gewählte Passwort. Ihre E-Mail-Adresse und Ihr Passwort sind Ihre Anmeldeinformationen.

Für die Nutzung kostenpflichtiger Dienste mit eingeschränktem oder personalisiertem Zugriff können auch zusätzliche obligatorische Daten angefordert werden, z. B. Ihr Geburtsdatum oder Ihr Titel (z. B. "Herr / Frau"), um Sie zur Einkaufsseite des zu leiten Zalando-Site, die Ihrem Geschlecht entspricht) oder Ihren Lieblingskleidungsstilen oder -marken.

Profildaten können auch zusätzliche Daten enthalten, die Ihre Person und Ihre Interessen betreffen. Diese können im Rahmen der Registrierung für den Dienst oder zu einem späteren Zeitpunkt erkannt werden. Dies ist beispielsweise der Fall, wenn Sie Ihrem Profil freiwillige Daten hinzufügen oder wenn Sie Ihr Kundenkonto verwenden möchten, um sich für einen Dienst zu registrieren, für den zusätzliche obligatorische Daten erforderlich sind.

**Rat**

Wenn Sie über Ihr Kundenkonto angemeldet sind, können Sie Ihre Daten anzeigen und in den meisten Fällen sogar direkt ändern, um beispielsweise Ihre Adresse nach einem Umzug zu aktualisieren.

**1.2 Kontaktdaten**

Wenn Sie mit uns Kontakt aufnehmen, erfassen wir Ihre Kontaktdaten. Abhängig davon, wie Sie uns kontaktiert haben (z. B. per Telefon oder E-Mail), können Ihre Kontaktdaten aus Ihrem Namen, Ihrer Postanschrift, Telefonnummern, Faxnummern, E-Mail-Adressen und Angaben zu Ihren Social-Media-Profilen bestehen ( Beispielsweise erhalten wir Ihre Facebook-ID, wenn Sie uns über Facebook kontaktieren), Benutzernamen und ähnliche Kontaktdaten.

**1.3 Kaufdaten**

Wenn Sie etwas bei Zalando bestellen oder vor Ort einkaufen, beispielsweise im Zalando Outlet Store, erfassen wir Ihre Kaufdaten. Die Kaufdaten können je nach Verkaufsart und Verarbeitungsstatus folgende Informationen enthalten:

* Bestellnummer;
* Angaben zu den gekauften Waren (Definition, Größe, Farbe, Kaufpreis usw.);
* Angaben zu den Zahlungsmitteln;
* Liefer- und Rechnungsadressen;
* Mitteilungen und Mitteilungen in Bezug auf Einkäufe (z. B. Widerrufserklärungen, Beschwerden und Mitteilungen an den Kundendienst);
* Liefer- und Zahlungsstatus, p. Ex. "Abgeschlossen" oder "Gesendet";
* Status der Rücksendung, p. Ex. "Erfolgreich beendet";
* Daten zu Drittanbietern, die an der Ausführung des Vertrags beteiligt sind (im Falle eines Versandhandels kann dies die Versandnummer des Kurierdienstes sein).

**Rat**

In den Bereichen "Meine Bestellungen", "Meine Retouren" und "Mein Adressbuch" Ihres Kundenkontos können Sie Ihre relevanten Kaufdaten jederzeit anzeigen.

**1.4 Zahlungsdetails**

Wir bieten Ihnen gängige Zahlungsmethoden im Online-Handel. Insbesondere sind dies die Vorauszahlung, die Kreditkarte, PayPal oder die Rechnung. Für die Ausführung der Zahlung erfassen wir die Zahlungsdaten, die Sie uns mitgeteilt haben. Wir erhalten zusätzliche Zahlungsdaten von externen Zahlungsverwaltungsdiensten und Wirtschaftsinformationsdiensten, mit denen wir zusammenarbeiten, um Zahlungen zu verwalten und die Kreditwürdigkeit zu überprüfen.

Zahlungsdaten können zum Beispiel sein:

* bevorzugte Zahlungsmittel;
* Rechnungsadressen;
* IBAN und BIC oder Kontonummer und Bankleitzahl;
* Kreditkartendetails;
* Solvabilitätsdaten;

Die Zahlungsdaten enthalten auch weitere Daten in unmittelbarem Zusammenhang mit dem Zahlungsvorgang und der Bonitätsprüfung. Hierbei handelt es sich beispielsweise um Daten, die externe Dienstleister zur Identifizierung verwenden, z. B. Ihre PayPal-ID (wenn Sie über PayPal bezahlen).

Die Zalando Payments GmbH, Mühlenstraße 13-19, 10243 Berlin, Deutschland, ist verantwortlich für das Zahlungsmanagement, die Kreditverwaltung und die Bonitätsprüfung in Bezug auf alle Einkäufe von Einzelpersonen im Zalando-Shop und für andere bezahlte Dienstleistungen der Zalando-Gruppe .

Die Bonitätsprüfungen bestehen aus Ihren eigenen Aufzeichnungen über Ihr bisheriges Zahlungsverhalten gegenüber allen Unternehmen der Zalando-Gruppe und aus Bewertungswerten für Sie, die wir von externen Wirtschaftsinformationsdiensten sammeln. Zu den Kreditwürdigkeitsdaten gehören Aussagen über die geschätzte finanzielle Leistungsfähigkeit und Verfügbarkeit einer Person. Dies ist nützlich für Unternehmen, um Forderungsausfälle zu vermeiden, die entstehen, wenn Kunden nicht zahlen oder zu spät zahlen können. Die Tatsache, dass wir bei der Auswahl der Zahlungsmittel auch Kreditwürdigkeitsdaten berücksichtigen, verhindert gleichzeitig, dass wir unseren Kunden Zahlungsmittel anbieten, die wir ihnen nicht anbieten können, und dass unsere Kunden Zahlungsverpflichtungen übernehmen, denen gegenüber sie können nicht erfüllen. Solvabilitätsdaten werden üblicherweise von sogenannten Wirtschaftsinformationsdiensten erhoben. Auf Basis verschiedener Daten berechnen die Wirtschaftsinformationsdienste den sogenannten Score-Wert, der unter anderem Folgendes berücksichtigt: bereits bestehende Zahlungsverpflichtungen und möglicherweise frühere Zahlungsschwierigkeiten. Score-Werte sind statistisch basierte Werte, die das zukünftige Risiko der Forderungsausfälle einer Person betreffen, und werden als numerischer Wert ausgedrückt, z. B. als Prozentsatz. Wir haben nur geringen Einfluss auf die Datenverarbeitung bei Wirtschaftsinformationsdiensten (z. B. wenn wir Daten über nicht ausgeführte Zahlungen an Wirtschaftsinformationsdienste übermitteln). Score-Werte sind statistisch basierte Werte, die das zukünftige Risiko der Forderungsausfälle einer Person betreffen, und werden als numerischer Wert ausgedrückt, z. B. als Prozentsatz. Wir haben nur geringen Einfluss auf die Datenverarbeitung bei Wirtschaftsinformationsdiensten (z. B. wenn wir Daten über nicht ausgeführte Zahlungen an Wirtschaftsinformationsdienste übermitteln). Score-Werte sind statistisch basierte Werte, die das zukünftige Risiko einer Forderungsausfall-Person betreffen, und werden als numerischer Wert ausgedrückt, z. B. als Prozentsatz. Wir haben nur geringen Einfluss auf die Datenverarbeitung bei Wirtschaftsinformationsdiensten (z. B. wenn wir Daten über nicht ausgeführte Zahlungen an Wirtschaftsinformationsdienste übermitteln).

Um den Besonderheiten und Anforderungen jedes Landes Rechnung zu tragen, erfolgt die Zusammenarbeit mit Zahlungsmanagementdiensten und Wirtschaftsinformationsdiensten speziell für jedes Land. Die Sektion[An wen werden meine Daten weitergeleitet?](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-10) meldet dabei Informationen über externe Zahlungsdienstleister [Länderspezifische Informationen](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-17)meldet Informationen zu den Informationsstellen, mit denen wir zusammenarbeiten. Dort finden Sie auch spezifische Hinweise zum Datenschutz, die wir Ihnen im Auftrag des jeweiligen Zahlungsmanagement- und Wirtschaftsinformationsdienstes zur Verfügung stellen.

**1.5 Zinsdaten**

Während Ihrer Interaktion mit unseren Diensten entstehen Daten, die es uns ermöglichen, die Inhalte, Themen, Produkte, Produktreihen, Marken oder Stile zu kennen, an denen Sie interessiert sind. Zum Beispiel können wir aus den Kaufdaten, dem Inhalt der Wunschliste, Ihrem Alter (sofern Sie uns diese Informationen zur Verfügung stellen) und durch Vergleiche mit anderen Benutzern mit ähnlichen Merkmalen die Stile und Produktkategorien ableiten, an denen Sie interessiert sind. Bei Ihrer nächsten Suche können wir Ihnen also zunächst die Produkte zeigen, die für Sie wahrscheinlich am relevantesten sind.

Zusätzlich zu den Interessen, die Sie uns direkt mitteilen, können wir Ihre Interessen auch aus anderen von uns gesammelten Daten extrapolieren. Wenn Sie sich beispielsweise wiederholt in einem bestimmten Bereich des Zalando-Shops anmelden, können wir im Rahmen der Nutzungsanalyse anhand Ihrer Zugangsdaten Rückschlüsse auf Ihre Interessen ziehen (z. B. wenn Sie regelmäßig die Kategorie "Sportswear" besuchen oder Wenn Sie Produkte dieser Kategorie bestellen, können wir daraus schließen, dass Sie wahrscheinlich an Sport interessiert sind.

Zu diesem Zweck erhalten wir von unseren externen Werbepartnern Daten und Statistiken zu demografischen Daten (Alter, Geschlecht, Region), Geräten und Zugangsdaten sowie zu den Interessen unserer Nutzer. Wir stellen sicher, dass unsere Werbepartner nur aggregierte, verschlüsselte oder anonymisierte Daten für Zalando übertragen, damit wir die Daten nicht einer bestimmten Person, insbesondere einem Benutzernamen, zuordnen können. Diese Informationen können uns helfen, unsere Benutzer besser zu verstehen.

Weitere Informationen zur Verarbeitung Ihrer Daten zu Werbezwecken finden Sie unter ["Wie verwendet Zalando meine Daten für Werbung?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-09).

**1.6 Mitteilungen, Interviewinhalte**

Wenn Sie mit uns oder anderen Benutzern telefonisch, per Post, über Social Media-Dienste, Kontaktformulare oder auf andere Weise über unsere Produkte (z. B. Produktbewertungen) oder andere Themen kommunizieren, erfassen wir den Inhalt Ihrer Kommunikation .

Bei Bedarf leiten wir Ihre Mitteilungen an die für Ihr Thema zuständigen Stellen weiter, möglicherweise an unsere Partnerunternehmen oder Produzenten. Im Falle einer Übertragung an ein anderes Unternehmen (z. B. wenn Sie uns Feedback an den Hersteller eines Produkts geben) haben Sie natürlich die Möglichkeit, uns mitzuteilen, dass Ihre Daten nur von Zalando verwendet werden sollen. In diesem Fall geben wir Ihre Mitteilung nicht oder nur ohne Ihre personenbezogenen Daten an die zuständige Stelle weiter, wenn Ihre Anfrage auf diese Weise bearbeitet werden kann.

Wenn Sie uns Mitteilungen für andere Benutzer über die dafür vorgesehenen Stellen senden (z. B. Produktbewertungen), können diese von uns im Rahmen unserer Dienstleistungen veröffentlicht werden.

**Aufzeichnung von Telefoninterviews**

Wir zeichnen Telefongespräche, beispielsweise mit unserer Hotline, nur auf, wenn Sie uns Ihre Erlaubnis dazu erteilen, und zwar nur für die in Ihrer Einwilligung enthaltenen Zwecke (z. B. Qualitätskontrolle, Schulung). Die Zustimmung zur Aufzeichnung von Interviews ist selbstverständlich freiwillig. Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen, indem Sie beispielsweise den Mitarbeiter auffordern, die Registrierung zu beenden. Weitere Informationen finden Sie unter der Überschrift ["Welche Datenschutzrechte habe ich?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-11).

Für die Kommunikation mit Kunden und Nutzern nutzt Zalando auch Angebote aus sozialen Netzwerken wie Facebook, Instagram oder Twitter. Wir nutzen diese Kommunikationsplattformen, um Ihnen neben unseren Kommunikationskanälen weitere Kontakt- und Informationsmöglichkeiten zu bieten. Bitte beachten Sie jedoch, dass wir nicht die Möglichkeit haben, in die Nutzungsbedingungen sozialer Netzwerke und die von ihnen angebotenen Dienste einzugreifen, und dass wir einen begrenzten Einfluss auf deren Datenverarbeitung haben. Wir bitten Sie daher, sorgfältig zu prüfen, welche personenbezogenen Daten Sie uns über soziale Netzwerke übermitteln. Wir haben keine Möglichkeit, das Verhalten der Manager sozialer Netzwerke, anderer Benutzer oder Dritter zu beeinflussen, die möglicherweise mit den Managern sozialer Netzwerke zusammenarbeiten oder deren Dienste nutzen.

**1.7 Daten sozialer Netzwerke**

Zalando verwaltet Profilseiten (auch "Fanseiten" genannt) in verschiedenen sozialen Netzwerken. Darüber hinaus können die Zalando-Dienste Funktionen für soziale Netzwerke wie Messaging-Dienste und sogenannte soziale Plug-Ins oder soziale Anmeldungen wie die Funktion "Mit Facebook anmelden" enthalten. Wenn Sie über unsere Social-Media-Profile in direktem Kontakt mit uns stehen oder die in unseren Diensten integrierten Funktionen des sozialen Netzwerks nutzen und Mitglied des jeweiligen sozialen Netzwerks sind, können wir vom Betreiber des betreffenden sozialen Netzwerks Daten erhalten, mit denen wir Sie identifizieren können. . In der Regel,

* Ihre öffentlichen Profilinformationen, die im jeweiligen sozialen Netzwerk gespeichert sind (z. B. Name, Profilfoto)
* Details zum verwendeten Gerätetyp
* Die Konto-ID Ihres Profils im jeweiligen Netzwerk (z. B. Facebook-ID)

Bitte beachten Sie auch die Hinweise zur Verarbeitung von Daten sozialer Netzwerke in Bezug auf Funktionen sozialer Netzwerke unter "[Informationen zu Websites und Anwendungen](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-04)"ist"[Informationen auf Social Media Fanseiten](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-05)".

Zalando nutzt derzeit den Facebook-Messaging-Dienst und soziale Plug-Ins / Login für die folgenden sozialen Netzwerke:

* Facebook Ireland Ltd., 4 Grand Canal Square, Hafen von Grand Canal, Dublin 2, IrelandFacebook Inc., 1601 S. California Ave., Palo Alto, CA 94304, USA ("Facebook"). Der Link zu den Datenschutzbestimmungen von Facebook ist hier verfügbar:[Informationen zu Facebook-Daten](https://www.facebook.com/about/privacy/).
* Twitter Inc., 795 Folsom St., Suite 600, San Francisco, CA 94107, USA ("Twitter"). Der Link zu den Datenschutzbestimmungen von Twitter ist hier verfügbar:[Twitter-Datenschutzrichtlinie](https://twitter.com/privacy).
* Pinterest Inc., 635 High Street, Palo Alto, Kalifornien, USA ("Pinterest"). Den Link zu den Datenschutzbestimmungen von Pinterest finden Sie hier:[Pinterest Datenschutzbestimmungen](http://about.pinterest.com/privacy/).

**1.8 Standortdaten**

Für bestimmte Zwecke erfassen wir auch die aktuellen Standortdaten Ihres Geräts, wenn Sie unsere Dienste nutzen. In diesem Zusammenhang setzen wir zwei verschiedene Technologien ein.

Wenn Sie die Standortdienste Ihres Geräts in einer App, Website oder einem anderen Onlinedienst von Zalando genehmigt haben, verarbeitet Zalando die von Ihrem Gerät gesammelten und uns zur Verfügung gestellten Standortdaten, um Ihnen entsprechende Dienste bereitzustellen. am Ort.

**Beispiel**

Mit einigen unserer Apps können Sie Geschäfte in Ihrer Nähe anzeigen oder Ihnen Produkte anbieten, die für Ihren aktuellen Standort geeignet sind.

Wenn Sie einer Zalando-App erlauben, auf die Ortungsdienste Ihres Geräts zuzugreifen, wird Ihr Standort möglicherweise regelmäßig an uns übertragen (z. B. auch wenn Sie die App zu diesem Zeitpunkt nicht verwenden). Dies dient dazu, die Benutzererfahrung zu verbessern, indem beispielsweise standortbezogene Inhalte schneller geladen werden, wenn Sie die App an Ihrem Standort verwenden, oder um standortbasierte Push-Kommunikation anzuzeigen. Wir verwenden diese Daten nicht zum Erstellen von Bewegungsprofilen.

Darüber hinaus erfassen wir Standortdaten von der IP-Adresse Ihres Geräts (bis auf Stadtebene). Hierfür wird eine verkürzte dreistellige, anonymisierte IP-Adresse verwendet. Es kann nicht verwendet werden, um Ihre Internetverbindung oder Ihr Gerät zu identifizieren.

**Was ist eine IP-Adresse?**

Jedes mit dem Internet verbundene Gerät muss einen eindeutigen mehrstelligen Code erhalten (Beispiel: 193.99.144.85). Dieser Code wird als IP-Adresse bezeichnet.

Die ersten drei Ziffern der IP-Adresse sind normalerweise diejenigen, die der Region oder einem bestimmten Internetanbieter zugeordnet sind. Anhand der IP-Adresse können Sie den Standort Ihrer Internetverbindung grob ablesen.

Dieser Prozess (sogenannte Geolocation) wird von uns und vielen anderen Online-Shops beispielsweise zur Betrugsprävention verwendet, um verdächtige Bestellungen zu identifizieren (in bestimmten Situationen kann es verdächtig sein, wenn Sie Bestellungen über Ihr Kundenkonto von einer Adresse aus aufgeben IP eines Landes, aus dem Sie noch nie bestellt haben).

**1.9 Fotos und andere persönliche Inhalte**

Mit einigen unserer spezifischen Anwendungen für bestimmte Dienste können Sie Fotos oder andere persönliche Inhalte mit uns oder anderen Benutzern teilen, mit uns oder anderen Benutzern kommunizieren oder Dienste anpassen (z. B. indem Sie ein Foto in Ihr Profil hochladen und die Fotosuche der App verwenden Zalando oder wenn Sie mit einem Stylisten kommunizieren).

**1.10 Daten für Aktionen und Meinungsumfragen**

Wenn Sie an einem von Zalando vorgeschlagenen Angebot (z. B. einem Preisspiel) oder einer Meinungsumfrage (z. B. Umfragen zur Kundenzufriedenheit als Teil der Marktforschung) teilnehmen, geben Sie dies bitte an Daten über Ihre Person.

Zum Beispiel fragen wir in einem Gewinnspiel normalerweise nach Ihrem Namen und Ihrer E-Mail-Adresse, um Sie im Falle eines Gewinns kontaktieren zu können und um sicherzustellen, dass jeder Teilnehmer nur einmal am Wettbewerb teilnehmen kann.

Bei einigen Aktionen und Untersuchungen werden Sie möglicherweise auch um zusätzliche Daten gebeten. Dies kann der Fall sein, wenn wir eine Aktion in Zusammenarbeit mit einem Partner durchführen und der Partner Informationen über Sie benötigt, um Ihnen die Gewinne zur Verfügung zu stellen. In solchen Fällen informieren wir Sie immer separat über die angeforderten Daten und deren Verwendung bei uns.

**1.11 Anträge auf Beschäftigung**

Um Bewerbungen entgegenzunehmen und zu bearbeiten, verlassen sich die Unternehmen der Zalando-Gruppe auf das zentrale Managementsystem für Bewerbungen der Zalando SE.

So greifen Sie auf das Webportal des zentralen Managementsystems für Bewerbungen von Zalando zu: <https://jobs.zalando.com/>. Das zentrale Management-Management-System von Zalando verfügt über dienstspezifische Hinweise zur Datenverarbeitung, die Sie unter folgendem Link aufrufen können:[[https://jobs.zalando.com/de/privacy-policy/]](https://jobs.zalando.com/en/privacy-policy/).

**1.12 Gerätedaten und Zugriff**

Bei der Nutzung von Online- und mobilen Diensten ist es unvermeidlich, dass technische Daten generiert und verarbeitet werden, um die angebotenen Funktionen und Inhalte bereitzustellen und auf Ihrem Gerät anzuzeigen. Diese Daten werden als "Geräte- und Zugriffsdaten" bezeichnet und jedes Mal erstellt, wenn Sie Online- und mobile Dienste nutzen. Unabhängig davon, wer der Anbieter ist, werden diese Daten beispielsweise erstellt, wenn Folgendes verwendet wird:

* Websites
* Anwendungen
* Social Media Fanpage
* E-Mail-Newsletter (z. B. wenn Ihre Interaktion mit dem Newsletter registriert ist)
* Standortbezogene Dienste

Zalando sammelt Geräte- und Zugriffsdaten in den von Zalando selbst angebotenen Online- und Mobilfunkdiensten (z. B. Shop Zalando). Zweitens kann Zalando Geräte- und Zugriffsdaten von Online- und Mobilfunkdiensten anderer Unternehmen empfangen, sofern diese soziale Medien oder Werbepartner von Zalando sind oder an denselben Online-Werbenetzwerken (z. B. "Google Network") teilnehmen. Weitere Informationen finden Sie im Abschnitt "[Wie verwendet Zalando meine Daten für Werbung?](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-09)"ist"[Informationen zu Fanseiten in sozialen Medien](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-05)".

Geräte- und Anmeldedaten umfassen die folgenden Kategorien:

* Allgemeine Informationen zum Gerät, z. B. Daten zum Gerätetyp, zur Betriebssystemversion, zu Konfigurationseinstellungen (z. B. Spracheinstellungen, Systemberechtigungen), Internetverbindungseinstellungen (z. B. Netzwerkname) Mobiltelefonnummer, Verbindungsgeschwindigkeit) und die verwendeten Apps (z. B. Name und Version der App).
* Identifikationsdaten (ID) wie Sitzungs-ID, Cookie-ID, eindeutige Geräteseriennummern (z. B. Google-Werbe-ID, Apple Ad ID), Konto-IDs von Drittanbietern (sofern Sie soziale Medien verwenden) Plug-In oder Social Login oder Zahlung über PayPal) und andere gängige Internet-Technologien, um Ihren Webbrowser, Ihr Gerät oder eine bestimmte App-Installation erkennen zu können.

**Beispiel**

Wenn Sie den Push-Kommunikationsdienst einer Zalando-Anwendung aktivieren, erhalten Sie eine zufällig generierte und eindeutige Push-ID zur Identifizierung. Anschließend senden wir die Push-ID zusammen mit der an Sie gerichteten Push-Kommunikation an den Push-Server, damit dieser sie an das richtige Gerät weiterleiten kann, dh an Ihr Gerät.

* Greifen Sie auf Daten zu, die Apps und Webbrowser bei jedem Online-Zugriff auf Webserver und Datenbanken automatisch übertragen (im Rahmen der sogenannten HTTP-Anfrage). Dies besteht aus standardisierten Informationen über den angeforderten Inhalt (z. B. Dateinamen und Dateityp einer abgerufenen Datei) sowie weiteren Informationen zum Zugriff auf den Server (z. B. übertragenes Datenvolumen und Fehlercodes) Gerät (z. B. Gerätetyp, Betriebssystem, Softwareversionen, Geräteidentifikationen, IP-Adresse, zuvor besuchte Seite und Zeitpunkt des Zugriffs).

**Zeige weniger**

**2. Wofür verwendet Zalando meine Daten?**

Zalando behandelt Ihre Daten in Übereinstimmung mit allen geltenden Datenschutzgesetzen. Damit halten wir uns bei der Verarbeitung personenbezogener Daten selbstverständlich an die datenschutzrechtlichen Grundsätze. Daher verarbeiten wir Ihre Daten grundsätzlich nur zu den in dieser Datenverarbeitungserklärung erläuterten und zum Zeitpunkt ihrer Erfassung deklarierten Zwecken. Diese stehen im Vordergrund des Kaufprozesses und der Bereitstellung, Anpassung und Entwicklung sowie der Sicherheit unseres Service. Wir verwenden Ihre Daten auch in der

In diesem Kapitel teilen wir Ihnen mit, auf welcher Rechtsgrundlage wir Daten für die einzelnen Zwecke verarbeiten. Abhängig von der Rechtsgrundlage, auf der wir Ihre Daten verarbeiten, können bestimmte Datenschutzrechte entstehen - zusätzlich zu Ihren stets bestehenden Datenschutzrechten wie dem Auskunftsrecht. In bestimmten Fällen haben Sie beispielsweise das Recht, der Verarbeitung Ihrer Daten zu widersprechen. Weitere Informationen finden Sie unter der Überschrift["Welche Datenschutzrechte habe ich?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-11)

**2.1 Entwicklung des Kaufs und der Bereitstellung von Online-, lokalen und personalisierten Diensten**

Wir verarbeiten Ihre Daten jeweils im Rahmen der zur Vertragserfüllung und zur Erbringung und Ausführung weiterer von Ihnen angeforderten Leistungen, wie in der Datenverarbeitungserklärung beschrieben. Die Zwecke der jeweils erforderlichen Datenverarbeitung richten sich daher nach dem Zweck des jeweiligen mit Ihnen geschlossenen Vertrages (einschließlich unserer Allgemeinen Geschäftsbedingungen und gegebenenfalls unserer Allgemeinen Handelsbedingungen und der dienstspezifischen Nutzung) oder der von Ihnen angeforderten Dienstleistungen. Die Hauptziele sind:

* Bereitstellung, Personalisierung und Einstellung gemäß den Anforderungen unserer Dienste wie Zalando Shop und Zalon (einschließlich ihrer Websites, Apps und Geräte und Funktionen einschließlich anderer Plattformen);
* die Bereitstellung lokaler Dienste, p. Ex. Zalando Outlet Stores und Events auf Messen und Events;
* Ausführen von Client-Programmen wie p. Ex. Zalando Outlet Card und Zalando Plus;
* die Ausführung von Kaufverträgen und Kundendienstleistungen einschließlich Versand und Zahlung, Kreditmanagement und Management von Retouren, Beschwerden und Gewährleistungsfällen;
* die Bereitstellung von Nachrichten, Mitteilungen, Newslettern und anderen direkten Kommunikationsmitteln, soweit diese ein wesentlicher Bestandteil unserer vertraglichen Dienstleistungen oder der von Ihnen angeforderten Dienstleistungen sind.

**Beispiele**

Im Zalando Shop erhalten Sie Informationen zur Verfügbarkeit von Artikeln, die verkauft wurden und jetzt wieder verfügbar sind.

In unseren Apps können Sie über den Push-Service über bestimmte Ereignisse, Angebote oder andere Themen informiert werden.

Wenn Sie unserem Online-Shopping-Club Zalando Privé beitreten, erhalten Sie regelmäßig unseren Zalando Privé-Newsletter mit Informationen zu aktuellen Sonderangeboten.

* die Gewährleistung der allgemeinen Sicherheit, der Funktionsweise des Systems und der Stabilität unserer Dienste einschließlich der Abwehr von Angriffen.
* nonverbale Kommunikation mit Ihnen in technischen, sicherheits- und vertragsrelevanten Angelegenheiten (z. B. Betrugswarnungen, Sperrung von Kundenkonten oder Vertragsänderungen).
* die Vermittlung von Verträgen über unsere Handels- und Verkaufsplattformen, p. Ex. als Teil des Partnerprogramms von Zalando oder Zalando Wardrobe.
* die Ausgabe, Einlösung, Lieferung von Zalando-Gutscheinen.
* Laufen von Spielen mit Preisen und Aktionen.

Die Zahlungsabwicklung zum Abschluss von Kaufverträgen wird von der Zalando Payments GmbH sichergestellt. Zu diesem Zweck nutzt Zalando auch die Dienste externer Zahlungsdienstleister. Informationen zu externen Zahlungsdienstleistern finden Sie im Abschnitt [An wen werden meine Daten weitergeleitet?](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-10).

Zitierte Gesetze:

Soweit der Zweck die Ausführung eines mit Ihnen geschlossenen Vertrages oder die Erbringung einer von Ihnen angeforderten Dienstleistung ist, ist Rechtsgrundlage Artikel 6 Absatz 1 Buchstabe b DSGVO. Ansonsten ist Rechtsgrundlage Artikel 6 Absatz 1 Buchstabe f DSGVO, wo unsere berechtigten Rechte in den vorgenannten Zwecken liegen.

**2.2 Personalisierung des Einkaufs**

Wir verarbeiten Ihre Daten, um nützliche und bequeme Dienste bereitzustellen, die Ihren Anforderungen und Interessen am besten entsprechen. Da das Angebot des Zalando-Shops Hunderttausende von Produkten und Tausende von Marken umfasst, ist es erforderlich, dass wir die Inhalte und Produkte in einer Weise präsentieren, die den Anforderungen entspricht, damit Sie die Produkte finden, die Sie tatsächlich interessieren. Dies erfordert eine kundenspezifische Bewertung der Relevanz von Produkten und Inhalten.

Für die Personalisierung des Einkaufs bei Zalando verwenden wir Geräte- und Zugriffsdaten, die wir für die Analyse der Nutzung sammeln. Wir verwenden auch Geräte- und Zugriffsdaten, die wir von Partnern erhalten, während Sie den Zalando-Shop besuchen. Wenn Sie während Ihres Besuchs im Zalando Shop über Ihr Kundenkonto angemeldet sind, verwenden wir auch Profil-, Interessen- und Kaufdaten für die Personalisierung des Einkaufs. Wir nennen diese Art der Personalisierung des Einkaufs vor Ort Optimierung. Nur diese Einkaufsoptimierung ermöglicht es uns, Ihnen geeignete Suchergebnisse zu präsentieren. Produktvorschläge, Stiltipps und andere Inhalte, die Ihren tatsächlichen Interessen entsprechen. Ohne diese Personalisierung des Einkaufs, wie sie heutzutage von vielen Online-Shops als Standard übernommen wird, wäre die Suche nach den für Sie relevanten Produkten weniger bequem, länger und der Nutzen unseres Vorschlags geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Abgesehen davon, dass Ihnen dank der Personalisierung des Einkaufs interessante Inhalte schneller angezeigt werden. Stilberatung und andere Inhalte, die Ihren tatsächlichen Interessen entsprechen. Ohne diese Personalisierung des Einkaufs, wie sie heutzutage von vielen Online-Shops als Standard übernommen wird, wäre die Suche nach den für Sie relevanten Produkten weniger bequem, länger und der Nutzen unseres Vorschlags geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Nur dank der Personalisierung des Einkaufens werden Ihnen interessante Inhalte schneller angezeigt. Stilberatung und andere Inhalte, die Ihren tatsächlichen Interessen entsprechen. Ohne diese Personalisierung des Einkaufs, wie sie heutzutage von vielen Online-Shops als Standard übernommen wird, wäre die Suche nach den für Sie relevanten Produkten weniger bequem, länger und der Nutzen unseres Vorschlags geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Abgesehen davon, dass Ihnen dank der Personalisierung des Einkaufs interessante Inhalte schneller angezeigt werden. Ohne diese Personalisierung des Einkaufs, wie sie heutzutage von vielen Online-Shops als Standard übernommen wird, wäre die Suche nach den für Sie relevanten Produkten weniger bequem, länger und der Nutzen unseres Vorschlags geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Nur dank der Personalisierung des Einkaufens werden Ihnen interessante Inhalte schneller angezeigt. Ohne diese Personalisierung des Einkaufs, wie sie heutzutage von vielen Online-Shops als Standard übernommen wird, wäre die Suche nach den für Sie relevanten Produkten weniger bequem, länger und der Nutzen unseres Vorschlags geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Nur dank der Personalisierung des Einkaufens werden Ihnen interessante Inhalte schneller angezeigt. länger und der Nutzen unseres Vorschlags wäre geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Nur dank der Personalisierung des Einkaufens werden Ihnen interessante Inhalte schneller angezeigt. länger und der Nutzen unseres Vorschlags wäre geringer. Natürlich haben Sie trotz der Personalisierung des Einkaufs Zugriff auf alle Inhalte. Nur dank der Personalisierung des Einkaufens werden Ihnen interessante Inhalte schneller angezeigt.

**mehr wissen**

Wir haben weitere Informationen darüber gesammelt, wie die Personalisierung des Einkaufs auf Websites und Apps unter Sprache funktioniert ["Einkaufsanpassung"](https://www.zalando.it/zalando-informativa-sulla-privacy/#shopping).  
Weitere Informationen zur Funktionsweise personalisierter Zalando-Services finden Sie unter["Personalisierte Dienste"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-03).

Zitierte Gesetze:

Rechtsgrundlage für die Verarbeitung Ihrer Daten zur Personalisierung des Einkaufs im Rahmen personalisierter Dienstleistungen ist Artikel 6 Absatz 1 Buchstabe b DSGVO. Rechtsgrundlage für die Verarbeitung Ihrer Daten im Rahmen der Vor-Ort-Optimierung ist Artikel 6 Absatz 1 Buchstabe f DSGVO, wo unsere berechtigten Rechte in den vorgenannten Zwecken liegen.

**2.3 Forschung, maschinelles Lernen und künstliche Intelligenz**

Wir verarbeiten die über unsere Kunden gesammelten Daten für wissenschaftliche Forschung in für Zalando relevanten Bereichen. Dies sind insbesondere die Forschungsbereiche maschinelles Lernen, künstliche Intelligenz, Verarbeitung natürlicher Sprache und tiefes Lernen. Die Forschung bei Zalando konzentriert sich auf die Lösung realer Probleme des täglichen Online-Einkaufslebens und zielt darauf ab, das bestehende Serviceangebot zu verbessern und weiterzuentwickeln.

Dabei halten wir uns offensichtlich an wissenschaftlich anerkannte Datenschutzstandards. Dies bedeutet auch, dass wir Ihre Daten nur in zusammengefasster, anonymisierter oder pseudonymisierter Form zu Forschungszwecken verarbeiten, indem wir beispielsweise alle identifizierbaren Daten wie Ihren Namen durch andere Daten ersetzen.

**mehr wissen**

Weitere Informationen zum Thema Forschung und Wissenschaft bei Zalando finden Sie im Eintrag [Zalando Research](https://research.zalando.com/). Für einen Überblick über die derzeit bei Zalando Research laufenden Forschungsprojekte klicken Sie auf[Hier](https://research.zalando.com/welcome/mission/research-projects/).

Die Forschung bei Zalando umfasst folgende Bereiche:

* Entwicklung automatischer Lernmethoden, mit denen wir geschätzte Werte, Prognosen und Analysen hinsichtlich der Bedürfnisse und Interessen unserer Benutzer erhalten können;
* die Entwicklung technischer Lösungen für echte Kundenprobleme, mit denen unsere spezialisierten Abteilungen und Modehersteller bei ihren täglichen Aktivitäten konfrontiert sind (z. B. Schwierigkeiten bei der Suche nach geeigneten Produkten, Verringerung der Anzahl falscher Einkäufe, Ermittlung von Größen);
* die Entwicklung technischer Lösungen zur Optimierung kommerzieller und logistischer Prozesse;
* die Entwicklung technischer Lösungen zur Verbesserung und Entwicklung der Personalisierung des Einkaufs und der Betrugsprävention;
* die Registrierung von Patenten und die Veröffentlichung von Artikeln in der Fachpresse;
* Teilnahme an Forschungsgruppen mit privaten und öffentlichen Kooperationspartnern.

**Beispiel**

Die Schuhgrößenempfehlung im Zalando Shop verwendet einen von Zalando Research entwickelten Algorithmus für maschinelles Lernen. Für die Entwicklung des Lernalgorithmus analysierte Zalando Research die Kaufdaten mit Schuhbestellungen, die Ursachen für Rückgaben aufgrund der Größe und die Größendaten der verschiedenen Hersteller. Aus diesen Daten wurde ein Verfahren zur Empfehlung der Schuhgröße entwickelt, um vorherzusagen, welche Modelle zu groß oder zu klein sind.

Zitierte Gesetze:

Rechtsgrundlage für die Verarbeitung Ihrer Daten im Rahmen der oben beschriebenen Forschungszwecke ist Artikel 6 Absatz 1 Buchstabe f DSGVO, wo unsere berechtigten Rechte in den oben genannten Zwecken liegen.

**2.4 Betrugsprävention, Auswahl der Zahlungsmethoden und Bonitätsprüfung**

**Betrugsprävention**

Um das Risiko einer Verletzung der Datensicherheit zu vermeiden, werden die Daten unserer Kunden nur verschlüsselt übertragen. Dies gilt sowohl für die Bestellung als auch für die Verbindung über das Kundenkonto. Hierfür verwenden wir das SSL-Verschlüsselungssystem (Secure Socket Layer). Dank der Verschlüsselung sind die Daten für Dritte nicht lesbar. Um uns weiter vor externen Angriffen zu schützen, verwenden wir spezielle Sicherheitstechnologien, die unsere Systeme kontinuierlich überwachen und Anomalien sofort erkennen und melden. Wir schützen unsere Systeme auch durch technische und organisatorische Maßnahmen vor Verlust, Zerstörung, Zugriff, Manipulation oder Offenlegung Ihrer Daten durch Unbefugte. Auf diese Weise möchten wir das Risiko eines unbefugten Zugriffs so gering wie möglich halten. Letztendlich ist der Schutz Ihrer Daten für uns von größter Bedeutung. Trotzdem können auch wir - wie andere Unternehmen - keinen absoluten Schutz garantieren. Manipulation oder Offenlegung Ihrer Daten durch unbefugte Personen. Auf diese Weise möchten wir das Risiko eines unbefugten Zugriffs so gering wie möglich halten. Letztendlich ist der Schutz Ihrer Daten für uns von größter Bedeutung. Trotzdem können auch wir - wie andere Unternehmen - keinen absoluten Schutz garantieren. Manipulation oder Offenlegung Ihrer Daten durch unbefugte Personen. Auf diese Weise möchten wir das Risiko eines unbefugten Zugriffs so gering wie möglich halten. Letztendlich ist der Schutz Ihrer Daten für uns von größter Bedeutung. Trotzdem können auch wir - wie andere Unternehmen - keinen absoluten Schutz garantieren.

Wir wenden auch manuelle Methoden zur Betrugsprävention an, um uns und unsere Benutzer vor Missbrauch Ihrer Daten zu schützen, insbesondere durch betrügerische Bestellungen. Zu diesem Zweck sammelt und wertet die Zalando Payments GmbH während des Bestellvorgangs unter einem Pseudonym Ihre Geräte- und Zugriffsdaten (einschließlich IP-Adresse, Kennungen, Nutzungsverhalten), Kauf- und Zahlungsdaten (einschließlich Adressdaten) aus. und andere Kreditwürdigkeitsdaten von Wirtschaftsinformationsdiensten) sowie historische Daten von Änderungen Ihrer Profildaten (z. wenn die Lieferadresse kürzlich geändert wurde). Die resultierenden Datenreihen werden dann mit Ihren vorherigen Verwendungs- und Bestellgewohnheiten verglichen. Darüber hinaus wird ein Vergleich mit einer Reihe allgemeiner Daten durchgeführt, die aus allen bei Zalando (auch von anderen Unternehmen der Zalando-Gruppe) erteilten Bestellungen stammen, bei denen betrügerische Aktivitäten stattgefunden haben oder bei denen der Verdacht auf betrügerische Aktivitäten besteht. Dieser Vergleich dient dazu, Betrugsmuster zu identifizieren und durch Mustervergleich Identitätsmissbrauch und Betrug zu verhindern. Manchmal,

Nach Abschluss der Registrierung für das Kundenkonto übermittelt die Zalando Payments GmbH in unserem Namen Ihren Namen und die Adressen, die Sie uns in Ihrem Profil mitgeteilt haben, an externe Geschäftsinformationsdienste. Dies dient dazu zu überprüfen, ob die übermittelten Adressen tatsächlich registriert oder erreichbar sind. Typische Hinweise - oft in Kombination miteinander -, die einen Betrugsversuch wahrscheinlicher machen, sind:

* Die Lieferadresse wurde kurz vor der Bestellung geändert und / oder befindet sich in einer Region mit hohem Betrugsrisiko.
* Ihre Bestellung ist besonders wichtig und / oder umfasst Waren, die derzeit stark nachgefragt werden und / oder zu einem für Ihre Region ungewöhnlichen Zeitpunkt (z. B. nachts) aufgegeben werden.
* Für die Bestellung werden die Zahlungsmethoden Lastschrift auf dem Konto oder der Rechnung verwendet.
* Während der Bestellung gab es verdächtige Anmeldeversuche in Bezug auf Ihr Kundenkonto, dessen Modell auf einen automatisierten Vorgang hinweist.
* Ihr Kundenkonto wurde von einer verdächtigen IP-Adresse verwendet.
* Ihr Kundenkonto wurde von einem unbekannten oder verdächtigen Gerät verwendet.

Wenn unser Sicherheitssystem einen Betrugsversuch oder ein hohes Betrugsrisiko feststellt, wird das betroffene Verfahren zur manuellen Überprüfung an die Betrugsabteilung weitergeleitet. Unter Berücksichtigung des Betrugsrisikos werden angemessene vorbeugende Maßnahmen getroffen (z. B. vorübergehende Sperrung des Kundenkontos oder Einschränkung der angebotenen Zahlungsmethoden).

In einigen Ländern können die Dienste der Risk.Ident GmbH, Am Sandtorkai 50, 20457 Hamburg oder Threatmetrix 160 W. Santa Clara St., Suite 1400, San Jose, Kalifornien 95113 USA (zertifizierter Datenschutzschild) zur Verhinderung von Betrug verwendet werden. Die Dienste werden derzeit in Frankreich, den Niederlanden und Deutschland genutzt.

Diese Dienstleister sammeln und verarbeiten Daten mithilfe von Cookies und anderen Tracking-Technologien, um das vom Kunden verwendete Endgerät zu identifizieren und weitere Daten zur Nutzung der Website zu sammeln. Es besteht keine Zuordnung zu einem bestimmten Benutzer.

Im Rahmen eines Bestellvorgangs auf unserer Website rufen wir die Risikobewertung des Endgeräts des Benutzers aus der Datenbank des Dienstleisters auf. Bei dieser Bewertung von Betrugsversuchen wird unter anderem bewertet, ob das Endgerät über verschiedene Anbieter eine Verbindung hergestellt hat oder ob das Endgerät über eine sich ständig ändernde Georeferenzierung verfügt, wie viele Transaktionen über dieses Gerät ausgeführt werden und wenn eine Proxy-Verbindung verwendet wird.

Zitierte Gesetze:

Soweit der Zweck der Verarbeitung Ihrer Daten die Verhinderung von Betrug gegen Sie ist, ist Rechtsgrundlage Artikel 6 Absatz 1 Buchstabe b DSGVO. Darüber hinaus erfolgt die Verarbeitung Ihrer Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, basierend auf unserem Interesse und dem berechtigten Interesse anderer Benutzer an der Identifizierung und Verhütung von Betrug und der Identifizierung von Straftaten.

**Auswahl der Zahlungsmethoden**

Bevor die für einen Kauf verfügbaren Zahlungsmethoden angezeigt werden, führt die Zalando Payments GmbH eine Risikoprüfung durch und bewertet die mit einer Bestellung bei Zalando verbundenen Gemeinkosten. Zum Zwecke der Durchführung der Risikoanalyse werden die zuvor aufgezeichneten Daten zu Kauf, Zahlung, Kreditwürdigkeit, Daten zu Ihrem vorherigen Zahlungsverhalten und Ihre Profildaten (z. B. Nachname, Vorname, Rechnungsadressen) verwendet und Lieferung, E-Mail-Adresse, Geburtsdatum). Die Überprüfung und Bewertung erfolgt automatisiert anhand statistischer Werte zum Risiko der Nichtzahlung von Zahlungen in Bezug auf die von uns angebotenen Zahlungsmethoden. Im Rahmen der Risikobewertung überträgt die Zalando Payments GmbH Ihre Daten auch an externe Geschäftsinformationsdienste, um allgemeine Daten zur Bewertung zahlungsspezifischer notleidender Risiken (z. B. zur Plausibilität und Aktualität Ihrer Adressdaten) zu erhalten. ) sowie in Einzelfällen Angaben zur Solvabilität, p. Ex. auf unbezahlte Rechnungen und Umstände, die unmittelbar zur Gefahr einer Nichtzahlung führen (z. B. Insolvenz, Verlängerung wegen Zahlungsunfähigkeit). Welche Kreditwürdigkeitsdaten bei der Risikobewertung tatsächlich berücksichtigt werden, kann von Land zu Land unterschiedlich sein.

**beachten**

Hier finden Sie länderspezifische Informationen zu den in den verschiedenen Ländern in Auftrag gegebenen Wirtschaftsinformationsdiensten und zu den unter dem Artikel verwendeten Kreditwürdigkeitsdaten ["Länderspezifische Informationen"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-17).

Die Gesamtkosten der spezifischen Zahlungsmethode für Zalando und die Verfügbarkeit dieser Zahlungsmethode im jeweiligen Land werden ebenfalls in die Entscheidung über die vorgeschlagenen Zahlungsmethoden einbezogen. Infolgedessen ist es möglich, dass bestimmte Zahlungsmethoden, die mit hohen Kosten oder Risiken für uns oder hohen Rückgaberaten verbunden sind, Kunden nicht mehr angeboten werden, die Produkte überdurchschnittlich zurückgeben (z. B. Rückgaberaten über 70%) oder die nur kleine Aufträge ausführen. Die Anpassung der verfügbaren Zahlungsmethoden reduziert die Rücklaufquoten, was zu mehr Nachhaltigkeit und Kosteneffizienz führt. Gleichzeitig bleiben unsere Dienstleistungen für unsere Kunden nutzbar,

Das Forderungsausfallrisiko für jede Zahlungsmethode wird einzeln bewertet und durch einen geschätzten Wert ausgedrückt. Wenn die Risikoüberprüfung erfolgreich ist, können wir Ihnen alle von uns angebotenen Zahlungsmethoden anbieten. Andernfalls können wir Ihnen nur bestimmte Zahlungsmethoden anbieten. Folgende Faktoren beeinflussen die Verfügbarkeit einer Zahlungsmethode:

* Die Kombination aus Adresse und Name kann nicht gefunden werden. Dies kann auf Rechtschreibfehler, Umzüge, Heirat oder die Integration von Gemeinden in andere zurückzuführen sein.
* Sie haben eine Lieferadresse, Abholstation oder Firmenadresse angegeben, die sich von der Rechnungsadresse unterscheidet.
* Es sind noch Kredite gegen Sie ausstehend.
* In der Vergangenheit gab es Zahlungsstörungen in Bezug auf bestimmte Zahlungsmethoden.

Die Risikoüberprüfung bedeutet nicht, dass Ihnen keine Zahlungsmethoden angeboten werden. Wenn Sie mit den von uns angebotenen Zahlungsmethoden nicht zufrieden sind, können Sie uns dies per Brief oder E-Mail mitteilen[revoca@zalando.it](mailto:revoca@zalando.it). Wir werden die Entscheidung anhand Ihrer Meinung überprüfen.

Zitierte Gesetze:

Soweit Sie der oben beschriebenen Verarbeitung Ihrer Daten zur Auswahl der Zahlungsmethoden zugestimmt haben, ist Rechtsgrundlage Artikel 6 Absatz 1 Brief eines DSGVO (Einwilligung). Andernfalls ist Rechtsgrundlage Artikel 6 Absatz 1 Buchstabe f DSGVO auf der Grundlage unseres berechtigten Rechts, das Risiko eines Zahlungsausfalls zu verhindern.

**Angaben zum Widerrufsrecht**

Sie haben das Recht, jede Einwilligung zum Abrufen von Kreditwürdigkeitsdaten für die Auswahl der Zahlungsmethode zu widerrufen. Weitere Informationen finden Sie unter "Welche Datenschutzrechte habe ich?"

**Überprüfen Sie die Zahlungsfähigkeit**

Zusätzlich zu [Risikoüberprüfung](https://www.zalando.it/zalando-informativa-sulla-privacy/#payment)Die Zalando Payments GmbH verarbeitet Ihre Daten im Rahmen einer automatisierten Bonitätsprüfung, bevor Ihnen die für einen Kauf verfügbaren Zahlungsmethoden angezeigt werden. Diese Überprüfung dient der Verhinderung von Zahlungsausfällen und unserer Sicherheit, da Betrugsversuche und andere Straftaten identifiziert werden können.

Zusätzlich zu den der Zalando Payments GmbH zur Verfügung stehenden Daten werden Kreditwürdigkeitsdaten von externen Geschäftsinformationsdiensten in Form von Bewertungswerten verwendet. Score-Werte sind statistisch basierte Werte, die das zukünftige Risiko einer Forderungsausfall-Person betreffen, und werden als numerischer Wert ausgedrückt, z. B. als Prozentsatz. Zu diesem Zweck übermittelt die Zalando Payments GmbH in unserem Auftrag die für eine Bonitätsprüfung erforderlichen personenbezogenen Daten (in der Regel Ihren Vor- und Nachnamen, Ihre Adresse und Ihr Geburtsdatum) an den externen Wirtschaftsinformationsdienst. Bei der Überprüfung können die Adressdaten verwendet werden, um den Bewertungswert zu berechnen. Der Wirtschaftsinformationsdienst verwendet die von uns übermittelten Daten, um eine Bewertung Ihrer Kreditwürdigkeit anhand statistisch-mathematischer Methoden für die jeweilige Bestellung vorzunehmen.

**beachten**

Informationen zu den in Ihrem Land in Auftrag gegebenen Wirtschaftsinformationsdiensten finden Sie im Eintrag ["Länderspezifische Informationen"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-17). Wenn Ihr Land nicht aufgeführt ist, führen wir in Ihrem Land keine Bonitätsprüfungen durch.

Abhängig vom Ergebnis der Bonitätsprüfung, d. H. Ob sie positiv oder negativ ist, werden geeignete Zahlungsmethoden angezeigt, mit denen Sie den Kauf fortsetzen und abschließen können.

Wenn Sie mit diesem Verfahren nicht einverstanden sind, können Sie uns per Brief oder E-Mail benachrichtigen [revoca@zalando.it](mailto:revoca@zalando.it). Wir werden die Entscheidung unter Berücksichtigung Ihrer Sichtweise prüfen.

Zitierte Gesetze:

Rechtsgrundlage für die vorgenannte Bonitätsprüfung ist Artikel 6 Absatz 1 Buchstabe b DSGVO, da dies für die Durchführung der erforderlichen vorvertraglichen Maßnahmen erforderlich ist. Darüber hinaus erfolgt die Verarbeitung Ihrer Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO auf der Grundlage unseres Interesses und des berechtigten Interesses anderer Nutzer an der Verhinderung von Zahlungsausfällen, der Identifizierung und Verhinderung von Betrug und der Identifizierung. von kriminellen Handlungen.

**2.5 Übermittlung von Überziehungszahlungsdaten an Inkassodienstleister**

Wenn Sie trotz wiederholter Mahnungen keine noch offenen Rechnungen begleichen, können wir die für die Zuordnung der Zuordnung zu dieser Agentur erforderlichen Daten zum Zwecke der Kreditrückforderung an die Kreditwiederherstellungsagenturen übertragen. Alternativ können wir die Forderung einem Inkassobüro zuweisen, das die Forderung in seinem Namen geltend macht. Informationen zu den für Ihr Land zuständigen Inkassodiensten finden Sie unter "[Länderspezifische Informationen](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-17)".

Zitierte Gesetze:

Die Übertragung von Daten im Rahmen des Treuhandkredit-Rückforderungsdienstes ist Kunst. 6, Absatz 1 b) der DSGVO; Die Übermittlung von Daten im Rahmen der Überweisung erfolgt auf der Grundlage von Art. 6, Absatz 1 f) der DSGVO.

**2.6 Werbung und Marktforschung, Datenanalyse**

Wir verwenden Ihre Daten auch im Rahmen der Datenanalyse für Werbe- und Marktforschungszwecke. Dabei verfolgen wir hauptsächlich folgende Ziele:

* Segmentierung in verschiedene Ziel- und Nutzergruppen im Rahmen der Marktforschung;
* Kenntnis verschiedener Zielgruppen und ihrer jeweiligen Nutzungsgewohnheiten und ihrer Einkaufsinteressen;
* Erlangung von Kenntnissen über Demografie, Interessen, Kauf- und Nutzungsgewohnheiten unserer Nutzer sowie Vermarktung dieses Wissens im Rahmen von Werbedienstleistungen für Dritte;
* die rechtzeitige Identifizierung von Trends in der Mode- und Online-Shopping-Branche;
* die Ausführung von Werbung für Kunden, die sich bereits im Portfolio befinden;
* die Ausführung von Direktwerbung, beispielsweise durch Newsletter;
* die Planung, Durchführung und Kontrolle des Werbeergebnisses, das den Interessen der betroffenen Zielgruppen entspricht (personalisierte Werbung);
* Kenntnis darüber, wie unsere Dienste genutzt werden (Nutzungsanalyse);
* die Vermarktung des oben genannten Wissens im Rahmen von Werbedienstleistungen an Werbekunden.

**Information**

Werbedienstleistungen werden in Zalando auch von der Zalando Marketing Services GmbH angeboten. [Auf die Website der Zalando Marketing Services GmbH](https://zms.zalando.com/)

Je nach Verwendungszweck verwenden wir die bei uns gespeicherten Daten auch zur Datenanalyse. Für die Analyse des Kaufverhaltens unserer Kunden verwenden wir beispielsweise gruppierte (aggregierte), statistische, depersonalisierte (anonymisierte) Profildaten und Daten, die nur über Zwischenschritte (pseudonymisierte Profildaten) mit Personen abgeglichen werden können ) sowie Geräte- und Zugangsdaten, um Einkaufsverfahren durch Datenanalyse analysieren und rekonstruieren zu können.

Wir verarbeiten Daten auf der Grundlage einer Interessenbewertung, um unsere berechtigten Interessen oder die von Dritten zu sichern (dies können beispielsweise Werbepartner oder Wiederverkäufer sein, die am Zalando-Partnerprogramm teilnehmen). Das berechtigte Interesse von Zalando oder Dritten an der Datenverarbeitung ergibt sich aus dem jeweiligen Zweck und ist, sofern nicht anders angegeben, wirtschaftlicher und wettbewerbsorientierter Natur.

Zitierte Gesetze:

Soweit die Datenverarbeitung mit Ihrer Zustimmung erfolgt, ist Rechtsgrundlage Artikel 6 Absatz 1 Brief einer DSGVO (Zustimmung). Darüber hinaus erfolgt die Datenverarbeitung auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, wo unsere berechtigten Rechte in den oben genannten Zwecken liegen.

**2.7 Produkt- und Technologieentwicklung**

Wir verwenden Ihre Daten für die Entwicklung von Produkten und Technologien, einschließlich der Entwicklung und Verbesserung kundenspezifischer Dienstleistungen. Dabei verwenden wir aggregierte oder anonymisierte Daten sowie Algorithmen für maschinelles Lernen, die beispielhaft durch unsere Forschung entwickelt wurden und es uns ermöglichen, geschätzte Daten, Prognosen und Analysen in Bezug auf die Interessen unserer Benutzer zu erhalten. So können wir Apps entwickeln, die Ihnen Produkte anbieten, die auf Ihre Bedürfnisse und Ihren Stil zugeschnitten sind und zu Produkten passen, die tatsächlich Ihren Interessen entsprechen.

* die Entwicklung und Verbesserung personalisierter Dienste und Technologien für Datenanalyse, Werbung und personalisierten Online-Einkauf;
* die Entwicklung von Technologien und Konzepten zur Erhöhung der Internetsicherheit, zur Verhinderung von Betrug und zur Verbesserung des Datenschutzes, p. Ex. durch Pseudonymisierungs-, Verschlüsselungs- und Anonymisierungstechniken;
* die Entwicklung und Erprobung von Softwarelösungen zur Optimierung der notwendigen kommerziellen und logistischen Prozesse.

Zitierte Gesetze:

Rechtsgrundlage für die Verarbeitung Ihrer Daten im Rahmen der Produkt- und Technologieentwicklung ist Artikel 6 Absatz 1 Buchstabe f DSGVO, wo unsere berechtigten Rechte in den vorgenannten Zwecken liegen.

**2.8 Verwaltung und Optimierung von Verwaltungsprozessen**

Bei Bedarf übertragen und verarbeiten wir Ihre Daten zu administrativen und logistischen Zwecken sowie zur Optimierung von Geschäftsabläufen innerhalb der Zalando-Gruppe, um diese effizienter und rechtlicher zu verwalten und unseren vertraglichen und rechtlichen Verpflichtungen nachzukommen (z. Verpflichtung zur Aufbewahrung von Handels- und Steuerdokumenten). Innerhalb der Zalando-Gruppe werden viele Systeme und Technologien gemeinsam verwendet. Auf diese Weise können wir einen günstigeren, sichereren, harmonischeren und besser personalisierten Service anbieten.

**Beispiele**

* Wenn Sie über Ihr Kundenkonto (Anbieter: Zalando SE) eine Verbindung zu Zalon (Anbieter: Zalando Fashion Entrepreneurs GmbH) herstellen, gewährt die Zalando SE der Zalando Fashion Entrepreneurs GmbH bei Bedarf Zugriff auf die in Ihrem Kundenkonto gespeicherten Daten. Auf diese Weise können Sie Profil- und Kontaktdaten aufschreiben, ohne sie erneut eingeben zu müssen. Ihre Bestellungen werden dann von Ihrem Zalon-Stylisten zur Beratung verwendet.
* Wenn Sie sich an die Zalando-Kundendienstabteilung wenden, wird Ihre Anfrage an die Zalando-Kundendienst DACH SE & Co. KG weitergeleitet und dort bearbeitet. Innerhalb der Zalando-Gruppe ist die Zalando-Kundenbetreuung DACH SE & Co. KG für den Kundenservice im deutschsprachigen Raum verantwortlich. Soweit dies für die Beantwortung Ihrer Frage erforderlich ist, kann der Kundendienstmitarbeiter der Zalando-Kundendienst DACH SE & Co. KG auf Ihre bei anderen Zalando-Unternehmen gespeicherten Daten zugreifen.

Die Datenverarbeitung zum Verwalten und Optimieren von Verwaltungsprozessen umfasst beispielsweise auch folgende Zwecke:

* die Ausführung und Verbesserung des Kundendienstes;
* die Verhütung und Aufklärung von Verbrechen;
* Gewährleistung der Sicherheit und Funktionalität unserer IT-Systeme;

Zitierte Gesetze:

Rechtsgrundlage für die Verarbeitung Ihrer Daten im Rahmen der Verwaltung und Optimierung von Verwaltungsprozessen ist Artikel 6 Absatz 1 Buchstabe f DSGVO, wo unsere berechtigten Rechte in den vorgenannten Zwecken liegen. Soweit wir Ihre Daten aufgrund gesetzlicher Bestimmungen aufbewahren, p. Ex. Die Rechtsgrundlage für die Aufbewahrung von Steuerunterlagen und für Kontrollen im Zusammenhang mit der Bekämpfung der Geldwäsche ist Artikel 6 Absatz 1 Buchstabe c DSGVO.

**2.9 Aufgrund Ihrer Zustimmung**

Wenn Sie der Verarbeitung personenbezogener Daten zugestimmt haben, ist die Rechtsgrundlage unserer Verarbeitung in erster Linie diese Einwilligung. Welche Daten wir aufgrund Ihrer Einwilligung verarbeiten, hängt in erster Linie vom Zweck Ihrer Einwilligung ab. Typische Zwecke sind zum Beispiel:

* einen Newsletter bestellen;
* Teilnahme an einer Umfrage oder Marktforschung;
* die Verarbeitung besonders sensibler Daten, aus denen beispielsweise Ihre politischen, religiösen oder ethischen Meinungen oder Ihr Gesundheitszustand abgeleitet werden können;
* die Aufzeichnung von Telefongesprächen, die Sie mit unserem Kundendienst führen;
* die Weitergabe Ihrer Daten an Dritte oder an ein Land außerhalb der Europäischen Union;
* Durchführung einer Bonitätsprüfung (sofern dies nicht zur Vertragserfüllung oder für vorvertragliche Maßnahmen erforderlich ist).
* Die Verarbeitung Ihrer Daten zu Ihrer Position erfolgt in bestimmten Fällen mittels Google Maps, um Ihnen z. Informationen zu den nächstgelegenen Sammelstellen für Ihre Bestellung.

**Angaben zum Widerrufsrecht**

Sie können die erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Dies kann passieren, p. Ex. per E-Mail, Post oder Fax.

Sofern der jeweilige Dienst die Funktion unterstützt, können Sie den Empfang von Newslettern und anderen Kommunikationsarten im Preference Center anpassen oder abbrechen. Den Link zum Preference Center finden Sie in jedem Newsletter. Darüber hinaus gibt es in jedem Newsletter eine Schaltfläche, mit der Sie den Newsletter abbestellen können.

Weitere Informationen finden Sie unter der Überschrift ["Welche Datenschutzrechte habe ich?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-11)

**2.10 Andere Zwecke**

Wenn das Datenschutzgesetz dies zulässt, dürfen wir Ihre Daten ohne Ihre Zustimmung auch für neue Zwecke verwenden, z. B. zur Durchführung von Datenanalysen oder zur Entwicklung unserer Dienste und Inhalte. Voraussetzung dafür ist, dass diese neuen Zwecke, für die die Verwendung der Daten vorgesehen ist, zum Zeitpunkt der Datenerhebung noch nicht festgelegt oder nicht vorhersehbar waren und dass die neuen Zwecke mit denen übereinstimmen, für die die Daten bestimmt sind wurden ursprünglich übernommen.

**3. Personalisierte Dienstleistungen**

Die Entwicklung und Bereitstellung kundenspezifischer Funktionen und Dienste hat für uns höchste Priorität. Unabhängig von Ort, Zeit und Art des verwendeten Geräts bieten wir Ihnen ein individuelles Einkaufserlebnis und ein auf Ihre individuellen Interessen zugeschnittenes Angebot. Die Verarbeitung Ihrer Daten zur Personalisierung unserer Dienstleistungen bei Zalando ist ein wesentlicher Bestandteil der Dienstleistungen.

**Beispiele**

* Wenn Sie auf Reisen mit der Zalando-App eine Wunschliste erstellen, können Sie diese auch auf der Zalando-Website öffnen und später bearbeiten.
* Wenn Sie auf der Zalando-Website nach einem Produkt suchen, speichern wir die Suchdaten. Auf diese Weise können wir Ihnen bei späteren Suchvorgängen auf der Website oder in der Zalando-App zunächst die Ergebnisse anzeigen, die für Sie wahrscheinlich am relevantesten sind.
* Wenn Sie ein Produkt in Ihren Warenkorb legen, können wir Sie basierend auf Ihren vorherigen Bestellungen und Rücksendungen bei der Auswahl der richtigen Größe beraten.
* Wenn Sie einen Newsletter bestellt haben, können wir Ihnen Produkte präsentieren, die an Ihre vorherigen Bestellungen angepasst sind.

**3.1 Was sind personalisierte Dienstleistungen?**

Durch personalisierte Dienstleistungen können wir Ihnen bessere, praktischere und sicherere Dienstleistungen anbieten. Zu diesem Zweck verwenden wir die gespeicherten Daten Ihrer Person, um Rückschlüsse auf Ihre Bedürfnisse und Interessen zu ziehen. Auf dieser Basis können wir Ihnen interessantere Inhalte anbieten, die Ihren Bedürfnissen und Interessen besser entsprechen. Natürlich haben Sie immer noch Zugriff auf alle Inhalte. Durch Personalisierung sehen Sie Inhalte, die für Sie interessant sind, schneller oder Inhalte werden speziell für Sie präsentiert (z. B. in Form einzelner Produktempfehlungen).

**3.2 Warum brauche ich ein Kundenkonto?**

Für die meisten unserer personalisierten Services muss ein Kundenkonto erstellt werden, damit wir die Daten, die wir über Sie sammeln, an einem zentralen Ort speichern können.

**3.3 Welche Daten werden auf meinem Kundenkonto gespeichert?**

Daten, die wir über Ihre Person sammeln, sowie Ihre Kundennummer (CustomerID) werden in Ihrem Kundenkonto gespeichert. Die Kundennummer ist eine zufällig generierte Folge von Nummern, die keine persönlichen Daten enthält. Ihre Daten werden mit Ihrer Kundennummer abgeglichen, um sie mit Ihrem Kundenkonto abgleichen zu können. Darüber hinaus fungiert die Kundennummer auch als Pseudonym.

**3.4 Welche Daten werden zur Personalisierung verwendet?**

Die Auswahl der personalisierten Inhalte erfolgt grundsätzlich auf der Grundlage aller in Ihrem Kundenkonto gespeicherten Daten.

Soweit Geräte- und Zugangsdaten verwendet werden, die nicht in Ihrem Kundenkonto gespeichert sind, werden diese nur für die jeweilige Personalisierung pseudonymisiert und für die Nutzungsdauer verwendet (d. H. Zum Beispiel in Bezug auf Ihre Kundennummer, jedoch nicht in Bezug auf Ihre Name oder andere sofort identifizierende Profildaten).

**Sie** werden **nicht** verwendet:

* Solvabilitätsdaten;
* Daten für Aktionen und Meinungsumfragen;
* Bewerbungen;
* Kommunikation (z. B. vom Kundendienst).

**3.5 Ihre Auswahl**

In Ihrem Kundenkonto können Sie jederzeit die meisten Daten anzeigen, die wir in Ihrem Kundenkonto gespeichert haben. Bei Bedarf können Sie auch die Daten in Ihrem Kundenkonto ändern und so die Personalisierung beeinflussen, indem Sie uns beispielsweise Ihre Präferenzen mitteilen.

Sofern die Personalisierung auf Geräte- und Zugriffsdaten basiert, können Sie die Erfassung dieser Daten verhindern, indem Sie die Erfassung dieser Daten durch Tracking-Tools deaktivieren. Beachten Sie in diesem Fall jedoch, dass Sie weniger personalisierte Services oder keinen personalisierten Service und Support erhalten. Bitte beachten Sie auch, dass die für personalisierte Dienste verwendeten Daten auch für andere Zwecke (einschließlich der Bereitstellung unserer Dienste) benötigt werden. Die Erfassung der zu diesem Zweck verwendeten Daten hört daher mit der Deaktivierung nicht auf.

**Zeige weniger**

**4. Informationen zu Websites und Apps**

Wir verwenden Ihre Daten, um die Zalando-Websites und -Apps verfügbar zu machen. Neben den Geräte- und Zugangsdaten, die bei jeder Nutzung dieser Dienste generiert werden, hängen die Art der verarbeiteten Daten und der Zweck der Verarbeitung insbesondere davon ab, wie Sie die über unsere Dienste zur Verfügung gestellten Funktionen und Dienste nutzen. Wir verwenden die Daten, die während der Nutzung unserer Dienste entstehen, auch, um herauszufinden, wie unser Online-Angebot genutzt wird. Wir verwenden diese Informationen unter anderem im Rahmen der Personalisierung von Einkäufen, zur Verbesserung unserer Dienstleistungen sowie zur personalisierten Werbung.

**4.1 Bieter**

Den für den Service verantwortlichen Anbieter finden Sie im Impressum der jeweiligen Website oder der jeweiligen App.

**4.2 Welche Daten werden gesammelt?**

Grundsätzlich erfassen wir alle Daten, die Sie uns direkt über unsere Dienste mitteilen.

**Geräte- und Zugriffsdaten**

Für jeden Zugriff auf unsere Server und Datenbanken werden Geräte- und Zugriffsdaten generiert und in sogenannten Server-Protokolldateien aufgezeichnet. Am Ende der jeweiligen Sitzung wird die darin enthaltene IP-Adresse kurzfristig anonymisiert, sobald der Speicher für die Aufrechterhaltung der Funktionalität der jeweiligen Website nicht mehr erforderlich ist.

Sofern es auf Ihrem Gerät verfügbar und aktiviert ist, erfassen wir auch den Identifikationscode Ihres Geräts (z. B. die sogenannte "Werbe-ID", wenn Sie ein Android-Gerät verwenden, oder die "Anzeigen-ID", wenn Sie ein Apple-Gerät verwenden). Dieser Gerätecode wird vom Hersteller des Betriebssystems Ihres Geräts angegeben und kann von Websites und Apps gelesen und verwendet werden, um Ihnen Inhalte basierend auf Ihren Nutzungsgewohnheiten zu präsentieren.

**Einloggen**

Für jeden Benutzer, der sich für ein Kundenkonto oder einen anderen Dienst registriert, erstellen wir ein passwortgeschütztes persönliches Login. Wenn Sie sich nach dem Anmelden mit Ihren Anmeldeinformationen nicht abmelden, bleiben Sie bei den meisten unserer Dienste automatisch angemeldet. Je nach Art des Dienstes wird hierfür ein Cookie oder eine vergleichbare Technologie verwendet. Mit dieser Funktion können Sie einen Teil unserer Dienste nutzen, ohne die Verbindung jedes Mal neu herstellen zu müssen. Aus Sicherheitsgründen werden Sie aufgefordert, Ihr Passwort erneut einzugeben, wenn Sie beispielsweise Sie möchten Ihre Profildaten ändern oder eine Bestellung aufgeben. Weitere Informationen finden Sie unter der Überschrift["Personalisierte Dienste"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-03).

**Soziales Plug-In**

Unsere Dienste können soziale Plug-Ins ("Plug-Ins") verschiedener sozialer Netzwerke enthalten. Mit Hilfe dieser Plug-Ins können Sie beispielsweise Inhalte teilen oder bestimmte Produkte anderen empfehlen. Plug-Ins sind normalerweise deaktiviert und übertragen daher keine Daten. Durch Klicken auf die entsprechende Schaltfläche (zB "Social Media aktivieren") können Sie die Plugins aktivieren. Mit einem weiteren Klick auf dieselbe Schaltfläche kann das Plug-In deaktiviert werden. Wenn das Plug-In aktiviert ist, Ihr Webbrowser stellt eine direkte Verbindung zum jeweiligen sozialen Netzwerk her. Der Inhalt des Plug-Ins wird direkt vom sozialen Netzwerk an Ihren Webbrowser übertragen und von diesem auf unserer Website eingefügt. Durch die Integration des Plug-Ins erhält das soziale Netzwerk die Informationen, die Sie auf der entsprechenden Seite unserer Website aufgerufen haben, und kann Ihr Gerät erkennen und auf Daten zugreifen. Wenn Sie im sozialen Netzwerk angemeldet sind, kann dieser Besuch mit Ihrem Konto im jeweiligen sozialen Netzwerk verknüpft werden. Wenn Sie mit den Plug-Ins interagieren, z. B. wenn Sie auf die Facebook-Schaltfläche klicken " Es ist möglich, dass Websites mit aktiviertem Social Plug-In Daten an Netzwerke übertragen. Bei jedem Aufruf einer Website wird über ein aktiviertes Plug-In ein Cookie mit einer ID eingefügt. Da Ihr Browser dieses Cookie überträgt, ohne bei jeder Verbindung mit dem Server des sozialen Netzwerks eine Bestätigung anzufordern, kann dieser im Prinzip ein Profil erstellen, welche Websites der mit dieser Identifikation verknüpfte Benutzer besucht hat. Darüber hinaus wäre es durchaus möglich, dass später, möglicherweise anlässlich einer späteren Verbindung mit dem sozialen Netzwerk,

**Facebook Social Plugin**

Auf unseren Websites verwenden wir Plug-Ins des sozialen Netzwerks facebook.com, das von Facebook Inc., 1601 S. California Ave., Palo Alto, CA 94304, USA ("Facebook") betrieben wird. Hier finden Sie den Link zur Facebook-Datenverarbeitungserklärung:[Facebook-Datenschutzhinweise](https://www.facebook.com/about/privacy/).

**Twitter Social Plug-In**

Auf unseren Websites verwenden wir Plug-Ins aus dem sozialen Netzwerk Twitter, das von Twitter Inc., 795 Folsom St., Suite 600, San Francisco, CA 94107, USA ("Twitter") betrieben wird. Hier finden Sie den Link zur Twitter-Datenverarbeitungserklärung:[Hinweise zum Datenschutz bei Twitter](https://twitter.com/en/privacy).

**Soziale Plugins von Pinterest**

Wir verwenden Plug-Ins aus dem sozialen Netzwerk von Pinterest auf unseren Websites, die von Pinterest Inc., 651 Brannan Street, San Francisco, CA 94103, USA ("Pinterest") betrieben werden. Hier finden Sie den Link zur Pinterest-Datenverarbeitungserklärung:[Pinterest Datenschutzhinweise.](https://policy.pinterest.com/en/privacy-policy).

**Social Login**

Schließlich bieten wir Ihnen in unseren Diensten die Möglichkeit, sich direkt bei uns in Ihrem Kundenkonto für soziale Netzwerke zu registrieren. Wenn Sie diese Funktion nutzen möchten, werden Sie zum Angebot des jeweiligen sozialen Netzwerks weitergeleitet. Sie werden aufgefordert, sich mit Ihren Anmeldeinformationen anzumelden. Offensichtlich nehmen wir Ihre Anmeldeinformationen nicht zur Kenntnis. Wenn Sie bereits registriert sind, wird dieser Schritt übersprungen. Das jeweilige soziale Netzwerk informiert Sie dann und bittet Sie um Bestätigung, welche Daten an uns übermittelt werden (z. B. öffentliches Profil, Freundesliste, E-Mail-Adresse und aktueller Wohnort). Mit den an uns übermittelten Daten erstellen wir ein Kundenkonto. Natürlich speichern wir Ihre Freundesliste nicht. Es besteht keine weitere dauerhafte Verbindung zwischen Ihrem Kundenkonto und Ihrem Konto in sozialen Netzwerken. Wir erhalten auch soziale Netzwerkdaten von den jeweiligen Anbietern sozialer Netzwerke.

**Einkaufsanpassung**

In unseren Diensten werden die Geräte- und Zugangsdaten, die sich aus der Analyse der Nutzung ergeben, die während der Nutzung entsteht, zur Personalisierung des Einkaufs verwendet. Je nach Art des Dienstes werden gängige Tracking-Technologien verwendet, die Tracking-Pixel und Identifikations-Cookies oder vergleichbare IDs (sogenanntes Tagging) verwenden. Auf diese Weise können unsere Werbepartner auch Ihr Gerät sammeln und auf Daten zugreifen, um uns Informationen über Ihre Interessen und demografischen Daten (z. B. Alter, Geschlecht, Region) während Ihrer Nutzung unserer Dienste zu liefern. Auf diese Weise können wir Ihnen spezifische Inhalte und / oder Angebote und Dienstleistungen präsentieren, deren Inhalt Ihren Interessen entspricht (z. B. Produktempfehlungen, die sich an der Tatsache orientieren, dass Sie sich in den letzten Tagen nur mit Sportschuhen befasst haben). Unser Ziel ist es, unser Angebot für Sie so attraktiv wie möglich zu gestalten und Ihnen Werbung zu präsentieren, die Ihren Interessengebieten entspricht. Natürlich können Sie weiterhin alle anderen Inhalte und Funktionen genießen. Diese Optimierung vor Ort ermöglicht es uns jedoch, Ihnen zunächst die Inhalte und Funktionen zu zeigen, die für Sie von größter Bedeutung sind. Die Optimierung vor Ort erfolgt automatisch in unseren Systemen, die erkennen, welche Benutzer die meisten Produkte und Inhalte einer bestimmten Kategorie aufgerufen haben.

**mehr wissen**

Weitere Informationen finden Sie unter der Überschrift ["Wie verwendet Zalando meine Daten für Werbung?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-09)

Wenn Sie keine Optimierung vor Ort wünschen, können Sie diese jederzeit deaktivieren:

* Deaktivieren Sie zu diesem Zweck im Zalando Shop die Funktion "Datenverarbeitung" (in der Zalando-App finden Sie diese Funktion im Informationsmenü unter "Über uns").

In anderen Diensten deaktivieren Sie zu diesem Zweck die Webanalyse oder App-Analyse.

Informationen zu Website-Cookies Unsere Websites verwenden Cookies. Die Annahme von Cookies ist keine Voraussetzung für den Besuch unserer Websites. Wir weisen jedoch darauf hin, dass unsere Websites möglicherweise eine eingeschränkte Funktionalität aufweisen, wenn Sie keine Cookies akzeptieren. Im Webbrowser können Sie festlegen, dass die Speicherung von Cookies nur erfolgt, wenn Sie damit einverstanden sind.

**Was sind Cookies?**

Cookies sind kleine Textdateien, die Ihr Browser speichert und die bestimmte Einstellungen und Daten für den Austausch mit unseren Webservern speichern.

Grundsätzlich werden zwei Arten von Cookies unterschieden: sogenannte Sitzungscookies, die gelöscht werden, sobald der Browser geschlossen wird, und permanente / temporäre Cookies, die über einen längeren Zeitraum gespeichert werden. Wir benötigen diesen Speicher, um die Websites und unsere Dienste so einrichten zu können, dass sie für Sie besser geeignet sind, und um Ihnen die Verwendung zu erleichtern, z. B. indem bestimmte Einstellungen gespeichert werden, sodass sie nicht jedes Mal wiederholt werden müssen.

Die von uns verwendeten Cookies können von Zalando oder von Werbepartnern stammen. Wenn Sie nur Cookies von Zalando akzeptieren möchten, nicht jedoch von unseren Werbepartnern, können Sie eine entsprechende Einstellung wählen (z. B. "Cookies von Drittanbietern blockieren" in Ihrem Browser). Normalerweise funktioniert die Hilfe in der Symbolleiste Ihres Webbrowsers erklärt, wie neue Cookies abgelehnt und bereits vorhandene unwirksam gemacht werden. Bei gemeinsam verwendeten Computern, die für die Annahme von Cookies und Flash-Cookies eingerichtet sind,

Wir verwenden drei Kategorien von Cookies für unsere Dienste:

* Notwendige Cookies: Diese Cookies sind für eine optimale Navigation und Nutzung der Website erforderlich. Mit diesen Cookies wird beispielsweise die Funktion des Warenkorbs realisiert. Auf diese Weise bleiben die Produkte im Einkaufswagen gespeichert, während Sie weiter einkaufen. Die erforderlichen Cookies werden auch verwendet, um bestimmte Einstellungen und Einträge zu speichern, die Sie vorgenommen haben, damit Sie sie nicht immer wieder wiederholen müssen, und um den Inhalt von Zalando an Ihre individuellen Interessen anzupassen. Ohne die erforderlichen Cookies kann die Website nicht verwendet werden oder ihre Nutzung ist eingeschränkt.
* Statistische Cookies: Diese Cookies sammeln Geräte- und Zugriffsdaten, um die Nutzung unserer Websites zu analysieren, z. B. welche Sektoren auf welche Weise verwendet werden (sogenanntes Surfverhalten), mit welcher Geschwindigkeit die Inhalte geladen werden und ob Fehler auftreten. Diese Cookies enthalten nur anonyme oder pseudonyme Informationen und werden nur verwendet, um unsere Websites zu verbessern und um zu wissen, was unsere Benutzer interessiert, sowie um die Wirksamkeit unserer Werbung zu messen. Statistische Cookies können blockiert werden,
* Marketing-Cookies ("Tracking-Cookie"): Diese Cookies enthalten Kennungen und sammeln Geräte- und Zugriffsdaten, um personalisierte Werbung auf der Zalando-Website auf Ihre individuellen Interessen abzustimmen. Unsere Werbepartner, die Online-Werbenetzwerke betreiben, sammeln auch Geräte- und Zugriffsdaten auf unseren Websites. Auf diese Weise können wir Ihnen auch personalisierte Werbung zeigen, die auf Ihre Interessen zugeschnitten ist, und zwar auf anderen Websites oder Apps anderer Anbieter (sogenanntes Retargeting). Marketing-Cookies können blockiert werden, ohne dass dies Auswirkungen auf die Navigation oder Nutzung der Website hat. Es ist möglicherweise nicht möglich, den Einkauf zu personalisieren.

Für den Zalando Shop haben wir länderspezifische Listen aller verwendeten Cookies zusammengestellt. Diese finden Sie unter der Überschrift["Hinweise auf einzelnen Websites"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-18).

**4.3 Über App**

**App Stores / Installation**

Die Zalando-Apps sind auf App-Plattformen verfügbar, die von Dritten betrieben werden, sogenannten App Stores (z. B. Google Play und Apple App Store). Falls erforderlich, erfordert der Download eine vorherige Registrierung im jeweiligen App Store. Zalando hat keinen Einfluss auf die Verarbeitung Ihrer Daten im Rahmen der Registrierung und Nutzung dieser App Stores. Daher ist der Betreiber des jeweiligen App Stores allein verantwortlich. Bei Bedarf wenden Sie sich bitte direkt an den Manager des jeweiligen App Stores.

**Inhalte teilen**

Wenn Ihr Betriebssystem über eine eigene Funktion zum Teilen von App-Inhalten verfügt, können Sie diese auch in unseren Apps über die Schaltfläche "Teilen" oder "Empfehlen" aufrufen, um Produkte zu empfehlen oder Inhalte zu teilen. Abhängig von den Funktionen Ihres Geräts oder Betriebssystems oder der Konfiguration Ihres Geräts können Sie auch soziale Netzwerke verwenden, um Inhalte freizugeben.

Bitte beachten Sie, dass es sich bei der Freigabefunktion unserer App um eine betriebssystemabhängige Funktion handelt. Wir erhalten keine Kenntnis von den Empfängern und Inhalten Ihrer Kommunikation. Weitere Informationen zur Freigabefunktion und ihren Konfigurationsoptionen erhalten Sie vom Hersteller Ihres Geräts.

Welche sozialen Netzwerke Ihnen zum Teilen von Inhalten zur Verfügung stehen, hängt davon ab, in welchem ​​sozialen Netzwerk Sie Mitglied sind und wie Sie Ihr Konto und Ihr Gerät für soziale Netzwerke konfiguriert haben. Weitere Informationen finden Sie in den jeweiligen Datenschutzerklärungen der von Ihnen genutzten sozialen Netzwerke.

**Standortbezogene Dienste.**

Die Funktionen einiger unserer Apps verwenden die Ortungsdienste Ihres Geräts, um Standortdaten zu erfassen. Dies geschieht ausschließlich, um Ihnen app-basierte Dienste und Inhalte anzubieten, die auf Ihren aktuellen Standort zugeschnitten sind. Eine App kann beispielsweise Geschäfte in Ihrer Nähe empfehlen und Ihnen Produkte anbieten, die an die klimatische Situation Ihres aktuellen Aufenthaltsortes angepasst sind. Wenn Sie der App den Zugriff auf Ortungsdienste erlauben, wird uns Ihr Aufenthaltsort regelmäßig mitgeteilt. Wir verwenden diese Daten nicht zum Erstellen von Bewegungsprofilen.

**Push-Service**

Unsere Apps benachrichtigen Sie möglicherweise über bestimmte Ereignisse oder Themen, auch wenn Sie die App zu diesem Zeitpunkt nicht aktiv nutzen. Push-Kommunikation ist eine spezielle Form von App-Messaging, mit der wir direkt mit Ihnen kommunizieren können. Wenn Sie dies nicht möchten, können Sie den Push-Dienst in den Einstellungen Ihres Geräts und in den Einstellungen innerhalb der App deaktivieren.

Wenn Sie den Push-Kommunikationsdienst aktivieren, wird Ihrem Gerät eine bestimmte Push-ID zugewiesen. Aus technischen Gründen können keine Push-Nachrichten ohne Push-ID gesendet werden. Push-IDs sind Kombinationen aus verschlüsselten und zufällig generierten Zahlen.

**Systemberechtigungen**

Für einige Funktionen müssen unsere Apps auf bestimmte Schnittstellen und Daten auf Ihrem Gerät zugreifen. Dies erfordert jedoch je nach verwendetem Betriebssystem eine spezielle Berechtigung. Im Folgenden erklären wir, welche Berechtigungen (soweit sie für die Verarbeitung Ihrer Daten relevant sind) unsere Apps möglicherweise benötigen und für welche Art von Funktionen sie erforderlich sind. Die Autorisierungseinstellungen können jederzeit in den Systemeinstellungen Ihres Geräts geändert werden.

* Standortdienste / Standortdaten: Damit eine App auf den von Ihrem Gerät erkannten Standort zugreifen kann, ist eine Berechtigung zum Zugriff auf die Standortdienste Ihres Geräts erforderlich. Wenn Sie einen solchen Zugriff nicht zulassen, ist die Anzeige von standortbezogenen Diensten möglicherweise nicht oder nur in begrenztem Umfang möglich.
* Messaging / Push-Messaging: Für die Nutzung von Push-Diensten ist eine Autorisierung erforderlich. Bei einigen Geräten ist die Autorisierung standardmäßig für alle Apps aktiviert.
* Zugriff auf gespeicherte Fotos: Damit eine App auf gespeicherte Fotos (Lesezugriff) und von der App erstellte Fotos zugreifen kann, um sie zu speichern (Schreibzugriff).
* Kamera: Für eine App ist eine Autorisierung erforderlich, um die Kamerafunktion Ihres Geräts zu verwenden, Fotos aufzunehmen oder QR-Codes zu lesen. Die jeweilige App greift nur auf die Kamera zu, wenn Sie eine entsprechende App-Funktion aufgerufen haben.
* Rufen Sie mobile Daten (iOS) auf oder rufen Sie den Zugriff auf alle Netzwerke und Netzwerkverbindungen (Android) auf: Bei Verwendung oder Installation einiger Apps werden diese Berechtigungen angefordert, damit die jeweilige App Daten über die Internetverbindung des Ihr Gerät (über WLAN oder Datenverbindung). Diese Berechtigung kann erforderlich sein, um die Daten zu übertragen, die Sie in die App eingeben, beispielsweise im Rahmen einer Suche auf unseren Servern.
* Löschen oder Ändern von Inhalten von USB-Speichern / SD-Karten und Lesen von Inhalten von USB-Speichern / SD-Karten: Diese Berechtigungen sind erforderlich, damit die jeweilige App Daten im Speicher oder in einem von Ihrem Gerät verwendeten zusätzlichen Speicher speichern und abrufen kann wenn erforderlich. Die jeweilige App liest nur Daten, die im Zusammenhang mit der Nutzung dieser App gespeichert wurden.

**4.4 Online-Werbung / Retargeting**

Unsere Websites und Apps enthalten Cookies und ähnliche Tracking-Technologien von Werbepartnern, die Online-Werbenetzwerke betreiben. Auf diese Weise können unsere Werbepartner auch auf Ihr Gerät zugreifen und auf Daten zugreifen und Ihnen personalisierte Werbung präsentieren, die auf Ihre Interessen zugeschnitten ist, auch auf den Websites und Apps anderer Anbieter (z. B. produktorientierte Werbung, die Sie haben gerade im Zalando-Shop gesehen).

Weitere Informationen finden Sie unter der Überschrift ["Wie verwendet Zalando meine Daten für Werbung?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-09)

Sie können die Verarbeitung Ihrer Daten für das Retargeting jederzeit deaktivieren:

* Deaktivieren Sie dazu die Funktion "Datenverarbeitung" im Zalando-Shop. In der Zalando-App finden Sie diese Funktion im Informationsmenü unter "Über uns". Im Zalando Web Shop finden Sie diese Funktion direkt neben dem Link, über den Sie zu dieser Datenverarbeitungserklärung gelangt sind.
* Deaktivieren Sie in anderen Diensten die Nutzungsanalyse.
* • Für andere Websites oder Apps können Sie das Retargeting auch durch teilnehmende Online-Netzwerke über die Deaktivierungsseite der European Interactive Digital Advertising Alliance (EDAA) deaktivieren: [Deaktivieren Sie weitere Werbung](http://www.youronlinechoices.com/it/le-tue-scelte/).

**4.5 Nutzungsanalyse**

Wir verwenden Tracking-Technologien in allen unseren Diensten, um Geräte zu bewerten und auf Daten zuzugreifen. Auf diese Weise können wir erfahren, wie unsere Benutzer unser Angebot im Allgemeinen nutzen. Hierbei werden Cookies und vergleichbare Kennungen verwendet. Auf diese Weise erfahren wir, welche Inhalte und Themen besonders gefragt sind, welche Seiten unserer Dienste am häufigsten verwendet werden, aus welcher Region (bis zur Stadtebene) unsere Dienste verwendet werden und im Allgemeinen welche Art von Browser und Gerät, das unsere Benutzer verwenden.

Darüber hinaus führen wir im Rahmen der Nutzungsanalyse gelegentlich A / B-Tests durch. A / B-Tests sind eine spezifische Variante der Fruchtanalyse. A / B-Tests (auch Split-Tests genannt) sind eine Möglichkeit, zwei Versionen einer Website oder App zu vergleichen, um herauszufinden, welche Version eine bessere Leistung erbringt oder den Benutzer dazu bringt, den gewünschten Inhalt schneller zu finden. . Durch das Erstellen und Testen der Versionen A und B werden Daten erhalten, auf deren Grundlage die Entscheidung über den Dienstwechsel einfacher und schneller getroffen werden kann.

Sie können per Spracheingabe sehen, welche Tracking-Tools auf unseren Websites und Apps verwendet werden ["Hinweise für einzelne Websites"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-18).

Dort finden Sie auch Warnungen zum Deaktivieren der Nutzungsanalyse.

Sie können die Verarbeitung Ihrer Daten zur Nutzungsanalyse jederzeit deaktivieren:

* Deaktivieren Sie dazu die Funktion "Datenverarbeitung" im Zalando-Shop. In der Zalando-App finden Sie diese Funktion im Informationsmenü unter "Über uns". Im Zalando Web Shop finden Sie diese Funktion direkt neben dem Link, über den Sie zu dieser Datenverarbeitungserklärung gelangt sind.
* Deaktivieren Sie in anderen Diensten die Nutzungsanalyse.

**Zeige weniger**

**5. Informationen zu Fanseiten in sozialen Medien**

Zalando besitzt Social-Media-Profile (sogenannte "Fanseiten") in den sozialen Netzwerken Facebook und Instagram. Wir veröffentlichen und teilen regelmäßig Inhalte, Angebote und Tipps auf unseren Fanseiten. Betreiber sozialer Netzwerke zeichnen Ihr Nutzungsverhalten durch Cookies und ähnliche Technologien bei jeder Interaktion auf unseren Fanseiten oder auf anderen Facebook- oder Instagram-Websites auf. Fanseitenbetreiber können allgemeine Statistiken zu den Interessen und demografischen Merkmalen (z. B. Alter, Geschlecht, Region) ihrer Besucher anzeigen. Bei der Nutzung sozialer Netzwerke werden Art, Umfang und Zweck der Datenverarbeitung hauptsächlich von den Betreibern der jeweiligen sozialen Netzwerke bestimmt.

**5.1 Anbieter / Verantwortlicher**

Das verantwortliche Zalando-Unternehmen, das als Inhaltsanbieter fungiert und eine Fanseite besitzt, kann in den rechtlichen Informationen der jeweiligen Fanseite eingesehen werden.

Die sozialen Netzwerke Facebook und Instagram werden beide von Facebook Ireland Ltd., 4 Grand Canal Square, Dublin 2, Irland ("Facebook") bereitgestellt.

Wenn Sie über unsere Fanseiten direkt mit uns kommunizieren oder persönliche Inhalte mit uns teilen, ist Zalando für die Verarbeitung Ihrer Daten verantwortlich. Eine Ausnahme bildet die nachfolgend beschriebene Verarbeitung von Daten zur Nutzungsanalyse (Page Insights); In diesem Fall sind wir zusammen mit Facebook verantwortlich.

**Verarbeitung Ihrer Daten durch Facebook**

Bitte beachten Sie, dass Facebook Ihre Daten auch verarbeitet, wenn Sie unsere Fanseiten für eigene Zwecke nutzen, die in dieser Datenschutzrichtlinie nicht erwähnt werden. Wir haben keinen Einfluss auf diese Facebook-Datenverarbeitungsvorgänge. Bitte beachten Sie hierzu die Datenschutzbestimmungen der jeweiligen sozialen Netzwerke:

* [Informationen zu Facebook-Daten](https://www.facebook.com/about/privacy/)
* [Instagram-Datenschutzrichtlinie](https://instagram.com/legal/privacy/)

**5.2 Welche Daten werden gesammelt?**

Wenn Sie unsere Fanseiten besuchen, sammelt Zalando alle Mitteilungen, Inhalte und sonstigen Informationen, die Sie uns direkt zur Verfügung stellen, beispielsweise wenn Sie etwas auf einer Fanseite veröffentlichen oder uns eine private Nachricht senden. Wenn Sie ein Konto im sozialen Netzwerk haben, können wir natürlich auch Ihre öffentlichen Informationen wie Ihren Benutzernamen, Informationen in Ihrem öffentlichen Profil und den Inhalt, den Sie als öffentlich teilen, anzeigen. Weitere Informationen finden Sie unter "[Welche Daten werden von Zalando verarbeitet?](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-01)".

**Nutzungsanalyse (Page Insight)**

Wenn Sie mit Fanseiten interagieren, verwendet Facebook Cookies und ähnliche Technologien, um das Nutzungsverhalten von Besuchen auf Fanseiten zu verfolgen. Auf dieser Basis erhalten Fanseitenbetreiber sogenannte "Page Insights", die nur statistische, depersonalisierte (anonymisierte) Informationen über die Besucher der Fanseite enthalten, die daher keiner bestimmten Person zugeordnet werden können. Wir haben keinen Zugriff auf die persönlichen Informationen, die Facebook zum Erstellen von Page Insights ("Page Insight-Daten") verwendet. Die Auswahl und

Page Insights geben uns Informationen darüber, wie unsere Fanseiten verwendet werden, was die Besucher von Fanseiten interessiert und welche Themen und Inhalte besonders beliebt sind. Auf diese Weise können wir die Aktivitäten der Fanseite optimieren, indem wir sie beispielsweise bei der Planung und Auswahl von Inhalten besser an die Interessen und Nutzungsgewohnheiten unseres Publikums anpassen.

Zalando und Facebook sind gemeinsam für die Verarbeitung Ihrer Daten für Page Insights verantwortlich. Zu diesem Zweck haben wir und Facebook eine Vereinbarung getroffen, welches Unternehmen seinen Datenschutzverpflichtungen aus der DSGVO hinsichtlich der Datenverarbeitung für Page Insights nachkommt.

**Erfahren Sie mehr über Page Insights**

Hier können Sie die Vereinbarung mit Facebook einsehen:  
<https://www.facebook.com/legal/terms/page_controller_addendum>

Facebook hat die wichtigen Teile dieser Vereinbarung (einschließlich einer Liste von Daten für Page Insights) für Sie hier zusammengefasst:  
<https://www.facebook.com/legal/terms/information_about_page_insights_data>

Rechtliche Grundlagen:

Wenn Sie der Erstellung von Page Insight-Daten für Facebook zugestimmt haben, ist Rechtsgrundlage Artikel 6 Absatz 1 der DSGVO (Zustimmung). Die Rechtsgrundlage ist im Übrigen Artikel 6 Absatz 1 der DSGVO, wonach unsere berechtigten Interessen für die oben genannten Zwecke gelten.

**5.3 Welche Rechte habe ich hinsichtlich des Schutzes personenbezogener Daten?**

Natürlich sind Ihre Datenschutzrechte unter "[Was sind meine Datenschutzrechte?](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-11)"gelten auch für die Datenverarbeitung in Bezug auf unsere Fanseiten.

Für die Verarbeitung Ihrer Page Insights-Daten mit Facebook haben wir mit Facebook vereinbart, dass Facebook in erster Linie dafür verantwortlich ist, Ihnen Informationen zur Verarbeitung Ihrer Page Insights-Daten zur Verfügung zu stellen und Ihnen die Ausübung Ihrer Datenschutzrechte gemäß der DSGVO zu ermöglichen ( z. B. Widerspruchsrecht). Weitere Informationen zu Ihren Rechten bezüglich des Schutzes personenbezogener Daten in Bezug auf Page Insights und wie Sie diese direkt auf Facebook ausüben können:  
<https://www.facebook.com/legal/terms/information_about_page_insights_data>

**6. Newsletter**

Wir bieten Ihnen verschiedene Newsletter-Services. Bei der Registrierung für den Newsletter-Service erhalten Sie Informationen zu den in den einzelnen Newslettern behandelten Themen und andere Hinweise. Darüber hinaus gibt es dienstspezifische Newsletter, die integraler Bestandteil eines bestimmten Dienstes sind. Beispielsweise erhalten Sie den Zalando Privé Newsletter nur, wenn Sie Mitglied des Zalando Privé Shopping Club sind. Bei Verwendung unseres Newsletters erfassen wir auch Geräte- und Zugriffsdaten.

**6.1 Wie registriere ich mich?**

Für den Versand unseres Newsletters mit Registrierungspflicht (wie den Newsletter aus dem Zalando Shop) verwenden wir das sogenannte Double-Opt-In- oder Single-Opt-In-Verfahren (je nach Land). Mit anderen Worten, wir senden Ihnen einen Newsletter erst, nachdem Sie uns ausdrücklich zur Aktivierung des Newsletter-Service autorisiert haben. Wenn in Ihrem Land das Double-Opt-In-Verfahren erforderlich ist, müssen Sie außerdem bestätigt haben, dass die von Ihnen angegebene E-Mail-Adresse Ihre ist. Zu diesem Zweck senden wir Ihnen eine Bestätigungs-E-Mail, mit der Sie um Bestätigung bitten, indem Sie auf einen in der E-Mail enthaltenen Link klicken. dass Sie der Eigentümer der uns mitgeteilten E-Mail-Adresse sind. Es ist möglich, dass wir auf diese Maßnahme verzichten, wenn Sie uns mit diesem Verfahren bereits zu einem anderen Zweck bestätigt haben, dass Sie der Eigentümer der uns mitgeteilten E-Mail-Adresse sind.

**6.2 Stornierung**

Wenn Sie unseren Newsletter später nicht mehr erhalten möchten, können Sie jederzeit widersprechen, ohne dass dies Kosten verursacht, die über die Übertragungskosten gemäß den Grundtarifen hinausgehen. Zu diesem Zweck ist eine Mitteilung in Textform (z. B. E-Mail, Fax oder Brief) an die jeweils für den Newsletter zuständige Firma Zalando ausreichend. Natürlich enthält jede Ausgabe des Newsletters auch einen Link zum Abbestellen.

**Melden Sie sich vom Zalando Shop Newsletter ab**

Wenn Sie den Zalando Shop-Newsletter abbestellen möchten, können Sie diesen Service auch bequem im Preference Center deaktivieren. Den Link zum Preference Center finden Sie in jeder Newsletter-E-Mail.

**6.3 Welche Daten werden gesammelt?**

Wenn Sie sich für einen Newsletter registrieren, speichern wir automatisch Ihre IP-Adresse sowie Datum und Uhrzeit der Registrierung und Bestätigung. Auf diese Weise können wir nachweisen, dass Sie sich tatsächlich registriert haben, und möglicherweise die unbefugte Verwendung Ihrer E-Mail-Adresse feststellen.

Wir sammeln Geräte- und Zugriffsdaten, die während Ihrer Interaktion mit einem Newsletter entstehen. Für diese Auswertung enthalten die Newsletter Links zu Bilddateien, die auf unserem Server gespeichert sind. Wenn Sie den Newsletter öffnen, lädt Ihr E-Mail-Programm diese Bilder von unserem Webserver herunter. Wir erfassen die Geräte- und Zugriffsdaten, die Sie in diesem Prozess bilden, in pseudonymisierter Form und unter einer zufällig generierten Kundennummer (Newsletter-ID), die wir ohne Ihre Zustimmung nicht zur Identifizierung verwenden. So können wir nachvollziehen, ob Sie den Newsletter geöffnet haben und welche Newsletter-Nummern Sie geöffnet haben. Die im Newsletter enthaltenen Links enthalten Ihre Newsletter-ID, damit wir herausfinden können, für welche Inhalte Sie sich interessieren. Mit den so erhaltenen Daten erstellen wir ein Benutzerprofil in Bezug auf Ihre Newsletter-ID, mit dem wir den Inhalt des Newsletters entsprechend Ihren Interessen und Ihren Nutzungsgewohnheiten personalisieren und die Nutzung unserer Benutzer durch unsere Benutzer statistisch analysieren können Newsletter. Wir kombinieren diese Daten nur mit den Daten, die wir im Rahmen der Nutzungsanalyse sammeln.

Diese Shopping-Personalisierung ist ein wesentlicher Bestandteil des Zalando Shop-Newsletters.

Sie können der Analyse des Newsletters jederzeit widersprechen, indem Sie den jeweiligen Newsletter-Service deaktivieren. Natürlich enthält jede Ausgabe des Newsletters auch einen Link zum Abbestellen. Weitere Informationen finden Sie unter der Überschrift["Welche Datenschutzrechte habe ich?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-11)

Alternativ können Sie auch die Anzeige von Bildern in Ihrem E-Mail-Programm deaktivieren. In diesem Fall kann der Newsletter jedoch nicht vollständig angezeigt werden.

**7. Produktempfehlungen per E-Mail und Push-Service**

Im Zusammenhang mit unseren Dienstleistungen präsentieren wir Ihnen Informationen und Angebote von Zalando basierend auf Ihren Interessen. Sie erhalten diese individuellen Produktvorschläge auch dann, wenn Sie keinen Newsletter abonniert haben. Für die Auswahl einzelner Produktangebote verwenden wir hauptsächlich Ihre Daten aus früheren Einkäufen und Ihre Daten von Interesse, aus denen wir Profil- und Interessendaten erhalten, die auf den Interessen und Präferenzen basieren, die uns gemäß den geltenden gesetzlichen Bestimmungen mitgeteilt wurden. .

Wenn Sie keine individuellen Produktvorschläge mehr von uns erhalten möchten, können Sie diesen Service jederzeit deaktivieren:

* Wenn Sie keine individuellen Produktangebote mehr von uns erhalten möchten, können Sie jederzeit informell widersprechen, ohne dass dies zusätzlich zu den Übertragungskosten gemäß den Grundtarifen (z. B. Internetverbindungskosten, Porto) zusätzliche Kosten verursacht, z Beispiel per E-Mail. Natürlich enthält jede E-Mail auch einen Link zum Abbestellen.
* Wenn Sie keine individuellen Produktangebote mehr von uns erhalten möchten, können Sie diese Funktion über den Push-Service jederzeit in den Einstellungen der jeweiligen App deaktivieren. In den meisten unserer Apps finden Sie die entsprechende Funktion im Bereich "Einstellungen" unter "Kommunikation" oder "Push-Kommunikation".

**8. Kaufen Sie Gutscheine**

Wir verwenden die im Rahmen einer Zalando-Gutscheinbestellung übermittelten Daten zur Überprüfung und Erfüllung der Bestellung sowie zum Versand und Einlösen des Gutscheins. Dies beinhaltet auch die Erfassung und Verarbeitung von Daten im Zusammenhang mit der Verwendung des Gutscheins, insbesondere zur Verhinderung von Betrug.

Zu diesem Zweck speichern wir auch folgende Daten:

* Ausstellungsdatum
* Wert des Gutscheins
* Coupon Code
* Personalisierungsdaten (wie von Ihnen angegeben)
* Name des Gutscheininhabers (in persönlichen Gutscheinen)
* wenn der Gutschein eingelöst wird
* Name des Sammlers und ID des Kundenkontos, das für die Sammlung verwendet wurde.

**9. Wie verwendet Zalando meine Daten für Werbung?**

Wir und unsere Werbepartner verwenden Ihre Daten für personalisierte Werbung, die Ihnen in den Zalando-Diensten sowie auf den Websites und Apps anderer Anbieter angezeigt wird. Zu diesem Zweck nutzen wir und unsere Werbepartner gängige Internet-Technologien auf dem Markt. Auf diese Weise können wir präziser werben und Ihnen nur Anzeigen und Angebote präsentieren, die für Sie so weit wie möglich relevant sind. Dies ermöglicht es uns, besser auf die Bedürfnisse der Personalisierung und Entdeckung neuer Produkte unserer Benutzer zu reagieren und sie durch ein persönliches Einkaufserlebnis langfristig für unsere Dienstleistungen zu interessieren.

**Beispiel**

Wenn Sie auf der Website eines Zalando-Werbepartners nach Sportschuhen suchen, können wir diese Informationen bei der Suche im Zalando-Shop berücksichtigen. So können wir Ihnen beispielsweise in der Produktkategorie "Schuhe" zunächst Sportschuhe zeigen oder Sportschuhe empfehlen, die bereits im Feed auf der Anmeldeseite enthalten sind. Wenn Sie uns Ihre Präferenzen im Kundenkonto mitteilen oder wenn Sie bereits Sportartikel bei uns gekauft haben, können wir diese Informationen auch in unseren Empfehlungen berücksichtigen.

**9.1 Werbeformate und -kanäle**

Die von Zalando und den Zalando-Werbepartnern verwendeten Werbeformate umfassen Präsentationen im Zalando-Shop (im Rahmen der Onsite- und In-App-Optimierung), Anzeigen in sozialen Netzwerken (z. B. Facebook-Anzeigen, Instagram-Anzeigen, YouTube-Videoanzeigen). und Werbeflächen, die von von Zalando verwendeten Online-Werbenetzwerken wie DoubleClick von Google verwaltet werden.

**Zalando Marketing Services GmbH**

Werbedienstleistungen werden in Zalando auch von der Zalando Marketing Services GmbH angeboten. [Auf die Website der Zalando Marketing Services GmbH](https://zms.zalando.com/)

Zalando verkauft keine persönlichen Daten. Wenn unsere Kunden ein Zalando-Werbeformat bei der Zalando Marketing Services GmbH anfordern, erhalten sie keine Daten, mit denen sie Sie ohne Ihre ausdrückliche Zustimmung direkt kontaktieren oder identifizieren können. Unsere Werbekunden erhalten nur anonyme und aggregierte Berichte mit Informationen über die Wirksamkeit und den Umfang der erbrachten Werbedienstleistungen. Diese Berichte basieren auf den Erkenntnissen der Zalando Marketing Services GmbH und berücksichtigen teilweise auch zusammengefasste Berichte, die wir von unseren Werbepartnern erhalten. Von ihnen können wir zum Beispiel sehen,

**9.2 Informationen, mit denen wir Zielgruppen definieren**

Für die Definition von Zielgruppen verwenden wir unser eigenes Wissen aus der Analyse des Nutzungs- und Kaufverhaltens unserer Kunden und Nutzer sowie aus unserer Marktforschung zur Marktsegmentierung, die wir auf die von Zalando erhobenen Nutzerdaten anwenden. Dabei berücksichtigen wir insbesondere aggregierte oder anonymisierte Kaufdaten, Suchpfade, Daten von Interesse und demografische Profildaten sowie Geräte- und Zugangsdaten.

**Beispiel**

Eine Zielgruppe könnte sein: "Frauen zwischen 25 und 35, modebewusst, sportinteressiert und haben in den letzten Jahren ein Adidas-Produkt bestellt".

Unsere Werbepartner haben auch die Möglichkeit, uns eigene Daten zur Benutzersegmentierung zur Verfügung zu stellen, die sie selbst sammeln. Werbepartner müssen sich verpflichten, nur aggregierte, verschlüsselte oder anonymisierte Daten für Zalando an uns zu übermitteln, damit wir die Daten nicht einer bestimmten Person, insbesondere einem bestimmten Benutzer des Zalando-Shops, zuordnen können. Für einige Zielgruppen wird die Zielgruppe auf der Grundlage der Surfverhaltensdaten der Benutzer definiert.

**9.3 Wie wir diese Informationen für Online-Werbung im Zalando-Shop und anderen Zalando-Diensten verwenden**

Wir verwenden die oben genannten Informationen im Rahmen der Optimierung vor Ort, um Ihnen relevantere Tipps und Inhalte zu präsentieren, wenn Sie nach einem Produkt suchen, Ihren Feed aufrufen oder einen Produktbereich besuchen. Die Onsite- und In-App-Optimierung basiert auf Cookies und vergleichbaren Identifikationstechnologien für die pseudonymisierte Erfassung von Geräte- und Zugriffsdaten. Diese Daten werden nicht dazu verwendet, Sie persönlich zu identifizieren, sondern nur zur pseudonymisierten Bewertung Ihrer Nutzung. Ihre Daten werden nicht dauerhaft mit anderen personalisierten Daten über Sie zusammengeführt, die bei uns gespeichert sind. Mit dieser Technologie können wir Ihnen Anzeigen und / oder spezifische Angebote und Dienstleistungen präsentieren, deren Inhalt auf Informationen basiert, die vom Gerät stammen, und auf Zugriffsdaten (z. B. Werbung, die darauf ausgerichtet ist, dass Sie in den letzten Tagen nur Gymnastikkleidung untersucht haben).

Wenn Sie keine Optimierung vor Ort wünschen, können Sie diese jederzeit deaktivieren:

* Deaktivieren Sie dazu die Funktion "Datenverarbeitung" im Zalando-Shop. In der Zalando-App finden Sie diese Funktion im Informationsmenü unter "Über uns". Im Zalando Web Shop finden Sie diese Funktion direkt neben dem Link, über den Sie zu dieser Datenverarbeitungserklärung gelangt sind.
* In anderen Diensten deaktivieren Sie zu diesem Zweck die Webanalyse oder App-Analyse. Bitte beachten Sie auch, dass die für die Optimierung vor Ort und in der App verwendeten Daten auch für andere Zwecke (einschließlich der Bereitstellung unserer Dienste) erforderlich sind. Die Erhebung der zu diesem Zweck verwendeten Daten endet daher nicht mit der Deaktivierung. Die Ihnen präsentierte Werbung wird nicht mehr personalisiert.

**9.4 in sozialen Netzwerken**

Wenn wir Werbung über die Werbeformate sozialer Netzwerke (z. B. YouTube, Facebook, Instagram) schalten, haben wir die Möglichkeit, Informationen über Benutzer von Zalando-Diensten (z. B. Geräte- und Anmeldedaten wie Cookie-IDs und Werbung, Adressen) zu übertragen E-Mail), von denen wir annehmen, dass sie Teil der Zielgruppe des Werbekunden sind oder wenn sie bestimmte Merkmale (z. B. Altersgruppe, Region, Interessen) in verschlüsselter Form für das jeweilige soziale Netzwerk aufweisen.

Das soziale Netzwerk entschlüsselt die von uns übermittelten Daten - entweder in unserem Namen als Vertragsabwickler oder mit Zustimmung des jeweiligen Nutzers - und präsentiert sie dem Nutzer (sofern dieser Mitglied des sozialen Netzes ist) im Rahmen seiner Beziehung Nutzung durch das jeweilige soziale Netzwerk, die von uns in Auftrag gegebene Werbung.

Wenn Sie nicht möchten, dass wir Ihre Daten verwenden, um Ihnen personalisierte Werbung in sozialen Medien zu präsentieren, können Sie die Übertragung Ihrer Daten deaktivieren:

* Deaktivieren Sie dazu die Funktion "Datenverarbeitung" im Zalando-Shop. In der Zalando-App finden Sie diese Funktion im Informationsmenü unter "Über uns". Im Zalando Web Shop finden Sie diese Funktion direkt neben dem Link, über den Sie zu dieser Datenverarbeitungserklärung gelangt sind.
* In anderen Diensten deaktivieren Sie zu diesem Zweck die Webanalyse oder App-Analyse.

Wenn Sie der Weiterleitung Ihrer Daten an soziale Netzwerke zugestimmt haben, können Sie Ihre Einwilligung jederzeit widerrufen.

Möglicherweise haben Sie auch die Möglichkeit, die Verwendung Ihrer Daten für personalisierte Werbung in den von Ihnen verwendeten sozialen Netzwerken direkt beim jeweiligen Betreiber zu deaktivieren. Für weitere Informationen wenden Sie sich bitte an die Manager:

Facebook (Facebook, Instagram):

* [Informationen zu Facebook-Anzeigen](https://www.facebook.com/about/ads/)
* [Anzeigeneinstellungen für Facebook](https://www.facebook.com/settings?tab=ads)

Google (Google-Werbenetzwerk, YouTube, Google-Suche):

* [Informationen zu Google-Anzeigen](https://policies.google.com/technologies/ads?hl=de)
* [Werbeeinstellungen für Google](https://adssettings.google.com/authenticated)

**9.5 auf Werbeflächen, die von Online-Werbenetzwerken betrieben werden (Retargeting)**

Werbepartner, die Online-Werbenetzwerke betreiben, können Cookies und ähnliche pseudonymisierte Tracking-Technologien für Ihr Nutzungsverhalten im Zalando-Shop, auf Zalando-Websites und in Apps anderer Anbieter auf der Grundlage von Geräte- und Zugriffsdaten verwenden. Diese Werbepartner verwenden diese gesammelten Daten, um die Wahrscheinlichkeit Ihrer Zugehörigkeit zur Zielgruppe zu erkennen und dies bei der Auswahl von Werbung über Werbeflächen zu berücksichtigen, die von Online-Werbenetzwerken betrieben werden. Diese Standard-Internet-Technologie wird als Retargeting bezeichnet.

Weitere Informationen erhalten Sie von den Betreibern der jeweiligen Werbefläche und von den für deren Verwaltung zuständigen Online-Werbenetzwerken. Eine Liste der Werbepartner und Opt-out-Hinweise finden Sie unter Eintrag["Hinweise für einzelne Websites"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-18).

Sie können die Verarbeitung Ihrer Daten für das Retargeting jederzeit deaktivieren:

* Deaktivieren Sie dazu die Funktion "Datenverarbeitung" im Zalando-Shop. In der Zalando-App finden Sie diese Funktion im Informationsmenü unter "Über uns". Im Zalando Web Shop finden Sie diese Funktion direkt neben dem Link, über den Sie zu dieser Datenverarbeitungserklärung gelangt sind.
* Deaktivieren Sie in anderen Diensten die Nutzungsanalyse.
* Für unsere Websites können Sie das Retargeting auch über teilnehmende Online-Netzwerke über die Opt-out-Seite der European Interactive Digital Advertising Alliance (EDAA) deaktivieren: [Deaktivieren Sie weitere Werbung](http://www.youronlinechoices.com/it/le-tue-scelte/).

Bitte beachten Sie auch, dass die für das Retargeting verwendeten Daten auch für andere Zwecke (einschließlich der Bereitstellung unserer Dienste) benötigt werden. Die Erhebung der zu diesem Zweck verwendeten Daten endet daher nicht mit der Deaktivierung. Die Ihnen präsentierte Werbung wird nicht mehr personalisiert.

**10. An wen werden meine Daten weitergeleitet?**

Zalando leitet Daten nur weiter, wenn dies nach deutschem oder gemeinschaftlichem Datenschutzrecht zulässig ist. Wir arbeiten besonders eng mit einigen Dienstleistungsunternehmen zusammen, beispielsweise im Kundendienstsektor (z. B. Hotline-Service), mit technischen Unternehmen (z. B. zur Verwaltung von Rechenzentren) oder mit Logistikunternehmen (z. zB Kuriere wie DHL). Diese Unternehmen dürfen Ihre Daten grundsätzlich nur unter besonderen Bedingungen und in unserem Auftrag verarbeiten. Soweit wir diese Unternehmen als beauftragte Verarbeitungsunternehmen beschäftigen, erhalten die Dienstleistungsunternehmen die Genehmigung dazu Zugriff auf Ihre Daten nur für den Umfang und für den Zeitraum, der für die Erbringung des jeweiligen Dienstes erforderlich ist. Wenn Sie bei einem Zalando-Partner einkaufen, geben wir bestimmte Ihrer Kaufdaten an den Zalando-Partner weiter (z. B. Ihren Namen und Ihre Lieferadresse), damit der Zalando-Partner die bestellte Ware an Sie liefern kann.

**10.1 Unternehmen der Zalando-Gruppe**

Innerhalb der Zalando-Gruppe werden viele Systeme und Technologien gemeinsam verwendet. Dies ermöglicht es uns, einen günstigeren, besseren, sichereren, harmonischeren und interessanteren Service anzubieten. Aus diesem Grund haben innerhalb der Zalando-Gruppe Unternehmen und Abteilungen, die diese zur Erfüllung unserer vertraglichen und rechtlichen Verpflichtungen oder zur Erfüllung ihrer jeweiligen Funktionen innerhalb der Zalando-Gruppe benötigen, Zugriff auf Ihre Daten.

**Beispiele**

* Wenn Sie über Ihr Kundenkonto (Anbieter: Zalando SE) eine Verbindung zu Zalon (Anbieter: Zalando Fashion Entrepreneurs GmbH) herstellen, gewährt die Zalando SE der Zalando Fashion Entrepreneurs GmbH bei Bedarf Zugriff auf die in Ihrem Kundenkonto gespeicherten Daten.
* Wenn Sie sich an den Zalando-Kundendienst wenden, wird Ihre Anfrage an den Zalando-Kundendienst DACH SE & Co. KG oder an den Zalando-Kundendienst International Se & Co. KG weitergeleitet und dort bearbeitet. Die beiden Unternehmen sind innerhalb der Zalando-Gruppe für den Kundenservice verantwortlich. Die beiden Zalando-Unternehmen können auf Ihre in anderen Zalando-Unternehmen gespeicherten Daten zugreifen, beispielsweise auf Ihre Bestelldaten, sofern dies für die Bearbeitung Ihrer Anfrage erforderlich ist.
* Wenn Sie eine Bestellung aufgeben, werden Ihre Bestell- und Zahlungsdaten an die Zalando Payments GmbH weitergeleitet. Innerhalb der Zalando-Gruppe ist die Zalando Payments GmbH für die Zahlungsabwicklung verantwortlich.

**10.2 Reedereien**

Wir arbeiten mit externen Dienstleistungsunternehmen (z. B. DHL) zusammen, um Bestellungen zu liefern. Diese Lieferfirmen erhalten von uns folgende Daten zur Erfüllung ihres jeweiligen Auftrags:

* dein Name;
* die Lieferadresse.
* möglicherweise Ihre Postnummer (wenn Sie eine Bestellung mit Lieferung an die Packstation aufgegeben haben);
* möglicherweise Ihre E-Mail-Adresse (wenn der Kurier Sie per E-Mail über die voraussichtliche Lieferzeit und das voraussichtliche Lieferdatum informieren möchte).

**10.3 Partner im Zalando-Partnerprogramm**

Im Rahmen des Zalando-Partnerprogramms ermöglichen wir anderen Händlern (sogenannten Zalando-Partnern), ihre Produkte (sogenannte Zalando-Partnerartikel) über den Zalando-Shop zu verkaufen. Im Rahmen des Zalando-Partnerprogramms dient der Zalando-Shop als Verkaufsplattform, über die Kaufverträge vermittelt werden. Unter dem jeweiligen Zalando-Partnerartikel sehen Sie den Text "Verkauf und Versand über unseren Partner" sowie den Namen des jeweiligen Zalando-Partners.

Wenn Sie einen Zalando-Partnerartikel bestellen, wird dieser normalerweise direkt vom jeweiligen Zalando-Partner versendet. Zu diesem Zweck geben wir Ihre Kaufdaten an den Zalando-Partner weiter. Diese schließen ein:

* Details zum jeweiligen Zalando-Partnerartikel;
* dein Name;
* die Lieferadresse.

In einigen Fällen, d. H. In einigen Ländern, geben wir Ihre E-Mail-Adresse oder Telefonnummer auch an einen Partner weiter. Dies geschieht jedoch nur, wenn dies erforderlich ist, um die Lieferung des Artikels an Sie zu ermöglichen.

Auch wenn Sie einen Artikel von einem Zalando-Partner bei Zalando kaufen, bleibt dieser für die Verarbeitung Ihrer Daten verantwortlich. Ihre Daten werden nicht gemeinsam mit einem Zalando-Partner oder im Auftrag eines Zalando-Partners verarbeitet. Zalando stellt sicher, dass der Zalando-Partner keine Kontrolle über die Verarbeitung Ihrer Daten innerhalb des Zalando-Partnerprogramms erhält. Wenn Sie Zalando-Artikel oder Zalando-Waren von einem Zalando-Partner kaufen, überträgt Zalando nur die oben aufgeführten Daten an den Zalando-Partner, die der Zalando-Partner benötigt, um seine Leistung Ihnen gegenüber zu erfüllen, d. H. normalerweise, um die von Ihnen bestellte Ware liefern zu können. Wenn Zalando Ihre Daten aus den oben genannten Gründen an einen Zalando-Partner übermittelt, stellt Zalando in den Vertragsbedingungen mit dem Partner sicher, dass Ihre Daten nur vom Zalando-Partner für die oben genannten Zwecke verarbeitet werden können.

Bitte beachten Sie, dass die Zalando-Partner ihre eigenen Datenschutzbestimmungen haben. Diese finden Sie normalerweise auf den jeweiligen Seiten der Zalando Shop-Partnerseiten und / oder auf den jeweiligen Seiten der Zalando-Partnerseiten. Zalando haftet nicht für die Datenverarbeitungsbestimmungen und Datenverarbeitungspraktiken der Zalando-Partner.

**10.4 Technische Dienstleistungsunternehmen**

Wir arbeiten mit Unternehmen zusammen, die technische Dienstleistungen anbieten, um Ihnen unsere Dienstleistungen anbieten zu können. Diese Unternehmen, die technische Dienstleistungen erbringen, sind die Telekom Deutschland GmbH, Salesforce.com EMEA Ltd. oder Amazon Web Services, Inc. Obwohl sie Ihre Daten außerhalb der Europäischen Union verarbeiten, kann dies dazu führen, dass Ihre Daten übertragen werden in einem Land mit einem Datenschutzstandard, der unter dem der Europäischen Union liegt.

**10.5. Zahlungsdienstleister**

Zalando bietet verschiedene Zahlungslösungen an, wie z. Vorauszahlung, Kreditkartenzahlung, Zahlung per PayPal und Rechnungszahlung. Zu diesem Zweck werden Zahlungsdaten an Zahlungsdienstleister weitergegeben, mit denen wir zusammenarbeiten. Weitere Informationen zur Verarbeitung personenbezogener Daten durch Zahlungsdienstleister finden Sie in den jeweiligen Datenschutzbestimmungen:

* **Adyen NV, Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam, Niederlande.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.adyen.com/policies-and-disclaimer/privacy-policy) von Ayden.
* **American Express Payment Services Limited, Niederlassung Frankfurt am Main, Theodor-Heuss-Allee 112, 60486 Frankfurt am Main.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.americanexpress.com/de/legal/online-datenschutzerklarung.html?inav=de_legalfooter_dataprivacy) von American Express Services Limited.
* **Elavon Financial Services DAC, eine Niederlassung in Deutschland, Lyoner Str. 36, 60528 Frankfurt am Main.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.elavon.co.uk/privacy-policy.html) von Evalon.
* **Worldpay BV Claude Debussylaan 16, 6. Stock, 1082 MD Amsterdam, Niederlande.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://online.worldpay.com/terms/privacy) von Worldplay.
* **iDeal von der Deutschen Bank AG, einer Niederlassung in den Niederlanden, De Entree 195, 1101 HE Amsterdam.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.db.com/company/en/data-protection.htm?kid=dataprotection.redirect-en.shortcut) der Deutschen Bank.
* **Svea Payments Oy, Mechelininkatu 1a, 00180 Helsinki.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.sveapayments.fi/terms-and-conditions-privacy-policies) von Svea Payments Oy.
* **BS PayOne von der PayOne GmbH, Lyoner Straße 9, 60528 Frankfurt am Main.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.payone.com/dsgvo/) von der PayOne GmbH.
* **PayPal (Europa) S.à rl et Cie, SCA, 22-24 Boulevard Royal, 2449 Luxemburg, Luxemburg.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.paypal.com/us/webapps/mpp/ua/privacy-full) per PayPal.
* **przelewy24 von PayPro Spólka Akcyjna, ul. Kanclerska 15, 60-327 Poznań und DialCom24 sp. z oo, ul. Kanclerska 15, 60-327 Poznań.**Weitere Informationen sind verfügbar [in der Datenschutzerklärung](https://www.przelewy24.pl/eng/information-obligation-gdpr-payer) von przelewy24.

**10.6. Wirtschaftsinformationsdienste**

Um den Besonderheiten und Anforderungen jedes Landes Rechnung zu tragen, erfolgt die Zusammenarbeit mit Wirtschaftsinformationsdiensten bei der Betrugsprävention, der Auswahl von Zahlungsmethoden und der Überprüfung der Kreditwürdigkeit spezifisch für jedes Land. Zum Artikel [Länderspezifische Informationen](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-17)Sie können sich über das Zahlungsmanagement und die Wirtschaftsinformationsdienste informieren, mit denen wir zusammenarbeiten. Dort finden Sie auch spezifische Hinweise zum Datenschutz, die wir Ihnen im Auftrag des jeweiligen Zahlungsmanagement- und Wirtschaftsinformationsdienstes zur Verfügung stellen.

**10.7 Inkassobüros**

Um den Besonderheiten und Anforderungen jedes Landes Rechnung zu tragen, erfolgt die Zusammenarbeit mit Kreditwiederherstellungsdiensten speziell für jedes Land. Unter Länderspezifische Informationen finden Sie Informationen zu den externen Inkassodiensten, mit denen wir in den jeweiligen Ländern zusammenarbeiten. Dort finden Sie auch spezifische Hinweise zum Datenschutz, die wir Ihnen im Auftrag der jeweiligen Inkassodienste zur Verfügung stellen.

**10.8 Social Media Netzwerke**

Im Rahmen von Werbekampagnen und in Übereinstimmung mit den gesetzlichen Datenschutzbestimmungen geben wir Daten an Anbieter des Social-Media-Netzwerks weiter. Weitere Informationen finden Sie unter der Überschrift["Wie verwendet Zalando meine Daten für Werbung?"](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-09).

**10.9 Öffentliche Stellen und andere Dritte**

**Zeige weniger**

**11. Welche Datenschutzrechte habe ich?**

Vorbehaltlich der jeweiligen gesetzlichen Bestimmungen haben Sie folgende gesetzliche Datenschutzrechte: Auskunftsrecht (Artikel 15 DSGVO), Recht auf Löschung (Artikel 17 DSGVO), Recht auf Berichtigung (Artikel 16 DSGVO), Recht auf Einschränkung der Verbreitung (Artikel 18 DSGVO) ), Recht auf Datenübertragbarkeit (Artikel 20 DSGVO), Recht auf Berufung bei einer öffentlichen Datenschutzbehörde (Artikel 77 DSGVO), Recht auf Widerruf der Einwilligung (Artikel 7 Absatz 3 DSGVO) sowie das Recht, gegen bestimmte Einwände zu erheben Maßnahmen zur Datenverbreitung (Artikel 21 DSGVO). Wenn Sie Ihre Rechte in Bezug auf die Datenverarbeitung geltend machen möchten, [revoca@zalando.it](mailto:revoca@zalando.it). Weitere Informationen finden Sie im Abschnitt[Kontakte](https://www.zalando.it/zalando-informativa-sulla-privacy/#chapter-15).

**Wichtige Hinweise:**

* Um sicherzustellen, dass Ihre Daten im Falle von **Informationsanfragen** nicht an Dritte weitergegeben werden, fügen Sie Ihrer Anfrage bitte einen geeigneten Identitätsnachweis bei und senden Sie ihn uns per Post oder E-Mail.

**Rat**

In der Regel reicht es aus, wenn Sie uns Ihre Anfrage unter Verwendung der in Ihrem Kundenkonto gespeicherten E-Mail-Adresse senden.

* Sie können die meisten im Kundenkonto enthaltenen Daten selbst ändern. In anderen Fällen wenden Sie sich bitte an den Kundendienst.
* Die Zuständigkeiten der öffentlichen Datenschutzbehörden richten sich nach dem Amt des jeweils zuständigen Amtes. Sie können sich jedoch auch an die öffentliche Datenschutzbehörde Ihres Wohnortes **wenden,** die Ihre **Beschwerde an** die zuständige öffentliche Stelle weiterleitet . Verantwortlich für Zalando ist der "Berliner Beauftragter für Datenschutz und Informationsfreiheit", Friedrichstr. 219, 10969 Berlin, Deutschland.
* Wenn Sie der Verarbeitung Ihrer Daten **zugestimmt haben** , können Sie diese **widerrufen** . Sie können es jederzeit widerrufen. Der Widerruf hat keine Auswirkung auf die Zulässigkeit der vor dem Widerruf vorgenommenen Verarbeitung Ihrer Daten.
* Sie können das **Objekt** für die Verarbeitung von Daten **Werbezwecke** , einschließlich der **Direktwerbung** (einschließlich in Form von Datenanalyse) jederzeit und ohne Angabe von Gründen .
* Wenn wir die Verarbeitung Ihrer Daten mit einer Zinsbewertung gemäß Artikel 6 Absatz 1 Buchstabe f DSGVO begründen (z. B. Meldung von Kreditwürdigkeitsdaten an einen externen Geschäftsinformationsdienst), können Sie **Berufung einlegen**gegen die Behandlung. Bitte erläutern Sie bei der Ausübung der Beschwerde die Gründe, warum wir Ihre Daten nicht verarbeiten sollten. Wenn der Einspruch gerechtfertigt ist, überprüfen wir die Situation und stellen die Verarbeitung Ihrer Daten ein oder passen sie an oder teilen unsere obligatorischen und geschützten Gründe mit, die es uns ermöglichen, die Verarbeitung fortzusetzen.

**12. Wann werden meine Daten gelöscht?**

Wir speichern Ihre personenbezogenen Daten so lange, wie dies für die Zwecke dieser Datenverarbeitungserklärung erforderlich ist, insbesondere zur Erfüllung unserer gesetzlichen und vertraglichen Verpflichtungen. Bei Bedarf werden wir Ihre personenbezogenen Daten auch für andere Zwecke speichern, sofern und solange das Gesetz es uns erlaubt, sie für bestimmte Zwecke weiter zu speichern, einschließlich zur Abwehr gesetzlicher Ansprüche.

Wenn Sie Ihr Kundenkonto schließen, werden alle über Sie gespeicherten Daten gelöscht. Wenn die vollständige Löschung Ihrer Daten nicht zulässig oder gesetzlich vorgeschrieben ist, werden die Daten für die weitere Verarbeitung gesperrt.

**Was bedeutet Blockieren?**

Durch die Sperrung von Daten wird durch die Einschränkung von Zugriffsrechten und anderen technischen und organisatorischen Maßnahmen sichergestellt, dass nur wenige Mitarbeiter auf die betreffenden Daten zugreifen können. Diese Mitarbeiter dürfen die Daten nur für vorgegebene Zwecke verwenden (z. B. im Fall einer Steuerprüfung zur Vorlage bei der Steuerverwaltung).

Das Sperren erfolgt beispielsweise in folgenden Fällen:

* Ihre Bestell- und Zahlungsdaten sowie möglicherweise andere Daten unterliegen verschiedenen gesetzlichen Aufbewahrungspflichten, die denen des Handelsgesetzbuches (in Deutschland HGB) oder der Steuervorschriften (in Deutschland AO. Ndt) entsprechen können. Das Gesetz verpflichtet uns zur Aufbewahrung Daten für steuerliche und wirtschaftliche Kontrollen für einen Zeitraum von zehn Jahren. Wir können die betreffenden Daten erst nach Ablauf dieser Frist endgültig löschen.
* Auch wenn Ihre Daten keiner Aufbewahrungspflicht unterliegen, können wir in den gesetzlich zulässigen Fällen auf eine sofortige Löschung verzichten und stattdessen zunächst eine Sperrung veranlassen. Dies gilt insbesondere für Fälle, in denen wir die fraglichen Daten möglicherweise zur weiteren Ausführung des Vertrags oder zur rechtlichen Verfolgung oder Rechtsverteidigung benötigen (z. B. im Falle von Beschwerden). Ausschlaggebend für die Dauer der Sperrung sind dann die gesetzlichen Verjährungsfristen. Nach Ablauf der jeweiligen Verjährungsfrist werden die Daten endgültig gelöscht.

In den gesetzlich vorgesehenen Fällen können wir von der Löschung abweichen, sofern es sich um anonymisierte oder pseudonymisierte Daten handelt und die Löschung dies unmöglich macht oder die Verarbeitung für wissenschaftliche Forschungszwecke oder statistische Zwecke ernsthaft beeinträchtigen würde.

**13. Wie schützt Zalando meine Daten?**

Bei uns werden Ihre persönlichen Daten sicher verschlüsselt übertragen. Dies gilt auch für Ihre Bestellung und Kundenanmeldung. Hierfür verwenden wir das SSL-Verschlüsselungssystem (Secure Socket Layer). Wir schützen unsere Webseiten und andere Systeme auch durch technische Maßnahmen vor dem Verlust, der Zerstörung, dem Zugriff, der Manipulation oder der Offenlegung Ihrer Daten durch unbefugte Personen.

**14. Änderungen dieser Erklärung zur Datenverarbeitung**

Während wir unsere Websites und Apps entwickeln und neue Technologien implementieren, um unsere Dienste für Sie zu verbessern, können Änderungen an diesen Datenschutzhinweisen erforderlich werden. Wir empfehlen Ihnen daher, diese Datenverarbeitungserklärung von Zeit zu Zeit zu lesen.

**15. Kontakte**

Unter "[revoca@zalando.it](mailto:revoca@zalando.it)"Sie können sich jederzeit an unser Datenschutz-Team wenden, um allgemeine Fragen zu stellen oder Ihre Rechte auszuüben.

Um unseren Datenschutzbeauftragten direkt zu kontaktieren, richten Sie Ihre Fragen bitte per Post an die unten angegebene Adresse mit dem Betreff "an den Datenschutzbeauftragten":

Datenschutz  
Zalando SE  
Valeska-Gert-Straße 5  
10243 Berlin  
Deutschland  
Telefax: +49 (0) 30 2759 46 93  
E-Mail:[revoca@zalando.it](mailto:revoca@zalando.it)

**16. Spezifische Informationen zum Service**

Die von uns durchgeführte Datenverarbeitung kann von Service zu Service unterschiedlich sein. Hier erfahren Sie, welche spezifischen Unterschiede bestehen.

**Zalon**

In Deutschland bieten wir unseren Kunden den sogenannten Sizer-Service an, der Sie über Ihre Maße informiert und es Ihnen erleichtert, die richtige Kleidung in der richtigen Größe zu finden. Wenn Sie diesen Service nutzen, werden wir Ihre Messungen anhand der Fotos vornehmen, die Sie uns senden. Bevor Sie Ihre Messungen vornehmen, machen wir Ihre Fotos durch Pixelierung und chromatische Inversion nicht wiederzuerkennen. Sobald die Messungen vorgenommen wurden, werden die Bilder gelöscht und die Daten gespeichert und an Sie übertragen, um die richtige Größe unserer Artikel zu kommunizieren und die Empfehlungen zur Eignung Ihrer Linie zu verbessern.

Die Verarbeitung erfolgt in Zusammenarbeit mit unserem israelischen Dienstleister Sizer Technologies Ltd., 22 Maskit St., Herzlia. Israel zählt zu den Ländern mit einem angemessenen Datenschutzniveau gemäß den festgelegten EU-Kriterien.

Rechtsgrundlage der Verarbeitung:

Wir verarbeiten Ihre Daten, um den von Ihnen angeforderten Dienst bereitzustellen (Artikel 6 Absatz 1 Buchstabe b DSGVO). Wir verarbeiten die Daten in aggregierter Form, um bessere Kenntnisse über Größen und Formen zu erhalten und den Service zu verbessern (Artikel 6 Absatz 1 Buchstabe f DSGVO).

**17. Länderspezifische Informationen**

Unsere Datenverarbeitung kann von Land zu Land unterschiedlich sein. Hier erfahren Sie mehr über die länderspezifischen Unterschiede.

**18. Hinweise zu Cookies**

Hier erfahren Sie, welche Cookies wir verwenden. Um auf die Übersicht aller Cookies zuzugreifen, klicken Sie hier [<https://www.zalando.it/cookies>]]

FACEBOOK

**Data Policy**

This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook ([Facebook Products](https://www.facebook.com/help/1561485474074139?ref=dp) or Products). You can find additional tools and information in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT39DaIrgbi_-ICyPEZnulHvMn0kVehM2Z-OYoz29Cq9mBYPYgSswa0a0cOv8G_wq2TLFFiP55RvIYv81TduLkK7txnWSLyNoTE39fC2JDtm4ZjmWLLBKtPQsU2qJsm-lEe0_rw-gemMM5ROdCCafQ).

**What kinds of information do we collect?**

To provide the Facebook Products, we must process information about you. The types of information we collect depend on how you use our Products. You can learn how to access and delete information we collect by visiting the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT0EwER5Q2qGjDUn0G2vZhbeCPTUkL-d_MNxL5iPq9si6Xlntp25t7qGqfJTDZY5a0R6B9Kr5NA-GfF3SWEt-Tv5Q9Jfz3kg2ici5KXN99wxJwZibe7FKhib1Aa8dnyLcKqNb6H2Djyza_7XCYedbA).

Things you and others do and provide.

* **Information and content you provide.** We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our [camera](https://www.facebook.com/help/162347444215311), so we can do things like suggest masks and filters that you might like, or give you tips on using portrait mode. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described [below](https://www.facebook.com/about/privacy/#how-we-use-information). Learn more about how you can control who can see the things you [share](https://www.facebook.com/help/1297502253597210?ref=dp).
  + Data with special protections: You can choose to provide information in your Facebook [profile fields](https://www.facebook.com/help/353111348061173?ref=dp) or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) is subject to special protections under EU law.
* **Networks and connections.** We collect information about the people, [Pages](https://www.facebook.com/help/282489752085908?ref=dp), accounts, [hashtags](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F351460621611097%3Fref%3Ddp&h=AT01BfllfNXWFSRCmOesbc09LnOVUXNVkMlbnoE2MQUCy4Da61RHafgQB4WYhJwizdbs9Qvbc9gqBzuA3pMmX-IjaVDSSrlGlSh1N2qf99TSC3AwhYQjqSTeiFLhJPOuGbDDpxa8pICrRRK3qLP8IQ) and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you [choose to upload, sync or import it from a device](https://www.facebook.com/help/561688620598358?ref=dp) (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed [below](https://www.facebook.com/about/privacy/).
* **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.
* **Information about transactions made on our Products.** If you use our Products for [purchases](https://www.facebook.com/help/1434403039959381?ref=dp) or other financial transactions (such as when you make a purchase in a game or make a [donation](https://l.facebook.com/l.php?u=https%3A%2F%2Fdonations.fb.com%2F&h=AT39E48kWark9dFDnnz4YC3W_ShUe9lwwf7nlzFDtlVmBQrHRcuAyY5qgEyJ3KWmZBizHr2vjffefrdetZNM6Mwbkb3xdH5LFg-VN8lGFUDLbJrbA7cNvDGxdDvMOuXV2IKwFMDHOLxxYMojB2tSHQ)), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
* **Things others do and information they provide about you.** We also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.

Device Information

As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including [ads](https://www.facebook.com/help/119468292028768?ref=dp)) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.  
  
Information we obtain from these devices includes:

* **Device attributes:** information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
* **Device operations:** information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
* **Identifiers:** unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to [Facebook Company Products](https://www.facebook.com/help/195227921252400?ref=dp) associated with the same device or account).
* **Device signals:** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
* **Data from device settings:** information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
* **Network and connections:** information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you [stream a video from your phone to your TV](https://www.facebook.com/help/276515126152168?ref=dp).
* **Cookie data:** data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the [Facebook Cookies Policy](https://www.facebook.com/policies/cookies/) and [Instagram Cookies Policy](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Flegal%2Fcookies%2F&h=AT1bWnTWlxiKXvaKYrETXYjQk6kcpdWuHkx08-cvNjMp7zUgABiCobB29xytqq88ifyF_9m3hlzCZSlw3dPLfQmE5b5Z66arEiE-YUiGcv62TzHUHAsMz6ixSvYJpATWEPmq5D9-6FnPIw5wTJBq2A).

Information from partners.

Advertisers, [app](https://www.facebook.com/help/1642635852727373?ref=dp) developers, and publishers can send us information through [Facebook Business Tools](https://www.facebook.com/help/331509497253087) they use, including our social plug-ins (such as the Like button), Facebook Login, our [APIs and SDKs](https://developers.facebook.com/docs/apis-and-sdks), or the Facebook [pixel](https://www.facebook.com/business/a/facebook-pixel). These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.  
  
Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. [Learn more](https://www.facebook.com/help/494750870625830?ref=dp) about the types of partners we receive data from.  
  
To learn more about how we use cookies in connection with Facebook Business Tools, review the [Facebook Cookies Policy](https://www.facebook.com/policies/cookies) and [Instagram Cookies Policy](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Flegal%2Fcookies%2F&h=AT3QxqZmj8__zzhwhgylElXMCkMWXjy-xQKAlMchxzwZYsJu3YcSuEb8XLjfayOw5onpdLFlzU7vEa9GSpjKeej_6lvbHpu_aI8FAdgmL0doZUAUSatAlml030r8_lQtufsVOJNxi-WqV8_vBnvR1A).

**How do we use this information?**

We use the information we have (subject to choices you make) as described below and to provide and support the Facebook Products and related services described in the [Facebook Terms](https://www.facebook.com/legal/terms/update) and [Instagram Terms](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F581066165581870%3Fref%3Ddp&h=AT0e706VWAM-BVOvMCBn-1Qa0OLX6f3TFuYRBghRGufSK-2ynETz-zMHnJXaNZ56cjypMFfSj1pgEmhkfwHkLnNAMCAJCbv0aGSsuXOpZe4Ni6UTRxZpCQ0fjUygUgIYe06aTkJ_KwYb2TT15TtvYw). Here's how:

Provide, personalize and improve our Products.

We use the information we have to deliver our Products, including to personalize features and content (including your [News Feed](https://www.facebook.com/help/166738576721085?ref=dp), [Instagram Feed](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F1986234648360433%3Fref%3Ddp&h=AT17lqyckIy5dJ19oiXKtHzgMk88yvFlok_aFatgEJyfJkbW8fWNAdb-FSi4B4cv6dV81ByRmv7yLsZxOn8EO2njkVJNSHoRs6xWi01T2c4VvDdltt1OHRdLFEo3y0WyHj76kAE5z2kGYCvr0igrpg), Instagram Stories and ads) and make suggestions for you (such as groups or [events](https://www.facebook.com/help/1076296042409786?ref=dp) you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any [data with special protections](https://www.facebook.com/about/privacy/#data-special-protections) you choose to provide where you have given your explicit consent); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products. Learn more about how we use information about you to personalize your Facebook and Instagram experience, including features, content and recommendations in Facebook Products; you can also learn more about how we choose the [ads](https://www.facebook.com/about/ads) that you see.

* **Information across Facebook Products and devices:** We connect information about your activities on different Facebook Products and devices to provide a more tailored and consistent experience on all Facebook Products you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger. We can also make your experience more seamless, for example, by automatically filling in your registration information (such as your phone number) from one Facebook Product when you sign up for an account on a different Product.
* **Location-related information:** We use [location-related information](https://www.facebook.com/about/basics/manage-your-privacy/location)-such as your current location, where you live, the places you like to go, and the businesses and people you're near-to provide, personalize and improve our Products, [including ads](https://www.facebook.com/about/ads), for you and others. Location-related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Facebook Products (such as check-ins or events you attend).
* **Product research and development:** We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.
* **Face recognition:** If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create are [data with special protections](https://www.facebook.com/about/privacy/#data-special-protections) under EU law. Learn more about [how we use face recognition technology](https://www.facebook.com/help/122175507864081?ref=dp), or control our use of this technology in [Facebook Settings](https://www.facebook.com/settings/facerec). If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.
* **Ads and other sponsored content:** We use the information we have about you-including information about your interests, actions and connections-to select and personalize ads, offers and other sponsored content that we show you. Learn more about how we [select and personalize ads](https://www.facebook.com/ads/preferences), and your choices over the data we use to select ads and other sponsored content for you in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT2CC0ri6ldH5PKbaC5FelHu1QNoeE9NNadDmgogE14bDnU9RG7cAnhA2YtxEmAAVyW5zvOKk3o1-hhvTOe9lo_iH-RaXsH-qifHHjj5-HIbs6K1BX5k8pQ7xaGDAQDLZ6GrcM4gVbAQqkLar2gCcg).

Provide measurement, analytics, and other business services.

We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services. [Learn how we share information](https://www.facebook.com/about/privacy/#sharing-partner-information) with these partners.

Promote safety, integrity and security.

We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to [detect when someone needs help](https://code.facebook.com/posts/286893341840510/under-the-hood-suicide-prevention-tools-powered-by-ai/). To learn more, visit the [Facebook Security Help Center](https://www.facebook.com/help/379220725465972?ref=dp) and [Instagram Security Tips](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F369001149843369&h=AT0Xtsd8sRsktI5UEJv8R3rP4f16CHpDgP8pIw8X90JnAh98r0L63i8GON2QXwmOfmVsFOBzzAZPmp0gffUOAMdCxlZd3gh1yb97KLAwQRO_kHGmwGv3ujd3mQKhi-_TlGM1lkcM2ZygwOsYpWJcIQ).

Communicate with you.

We use the information we have to send you marketing communications, communicate with you about our Products, and let you know about our policies and terms. We also use your information to respond to you when you contact us.

Research and innovate for social good.

We use the information we have (including from research partners we collaborate with) to conduct and support [research](https://l.facebook.com/l.php?u=https%3A%2F%2Fresearch.fb.com%2F&h=AT1RjI2nZ7xwH52aexXK9U6w_7aUZdH9uRj9YZ4ACADbzIDUfcRS87v0youNQ4WdcNyhfLwyXa2Aji-D0hqvDbTJP94EsvMYRUdAhh5OuyRBEFa2uq2QlZgW6oXRn3XoJXfWusLT-etdeVd91JBIDg) and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. For example, [we analyze information we have about migration patterns during crises](https://l.facebook.com/l.php?u=https%3A%2F%2Fresearch.fb.com%2Ffacebook-disaster-maps-methodology%2F&h=AT1OMWC6t6bS5QplwlgSVVBFm48oRh50khuVNCL_fAMDttM7X_YXmHvVz3E3s9cjDK8mRs0hjvia9jmzZQI7MG_f5CdCTxf3xTFx_iZNTXpYVJY-khvfSGZCdErfaR6EYk9Dh39FuhfoVqLU2zVt0w) to aid relief efforts. [Learn more](https://l.facebook.com/l.php?u=https%3A%2F%2Fresearch.fb.com%2F&h=AT0l8z6VU_nqBorlvGu7pdFru6rQ3F76gVrqM7pWqPXnPmPZkCr3QDF456OgkxvHe50ZdLk70lYvAX-rz34fps856Uzf-LNAscOcevbPr5ocryNy6pbqc1UvPlebbRUWS7i96Ww_GXF6z-FnWjbtDZEmmq14PqNnDXE) about our research programs.

**How is this information shared?**

Your information is shared with others in the following ways:

Sharing on Facebook Products

People and accounts you share and communicate with

When you share and communicate using our Products, [you choose the audience for what you share](https://www.facebook.com/help/120939471321735?ref=dp). For example, when you post on Facebook, you select the audience for the post, such as a group, all of your friends, the public, or a customized list of people. Similarly, when you use Messenger or Instagram to communicate with people or businesses, those people and businesses can see the content you send. Your network can also see actions you have taken on our Products, including engagement with ads and sponsored content. We also let other accounts see who has viewed their Facebook or Instagram Stories.  
  
[**Public information**](https://www.facebook.com/help/203805466323736?ref=dp) can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your [public profile on Facebook](https://www.facebook.com/help/203805466323736?ref=dp); and content you share on a Facebook Page, [public Instagram account](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F448523408565555%3Fref%3Ddp&h=AT2WrqibaU9uMl6aatB9JKZyVHhUY9UhxKGLNA27OlcjynDpgmTl1nrnVa_xpHoT2f5d9188U8iVlV3OsDrsZz-pxLGU2hO_Q70ZPxHaYy0UfVfocFVV4BlGxkRqkHCXpLgAfqvvdlsDWtYJBjHatQ) or any other public forum, such as [Facebook Marketplace](https://www.facebook.com/marketplace). You, other people using Facebook and Instagram, and we can provide access to or send public information to anyone on or off our Products, including in other Facebook Company Products, in search results, or through tools and APIs. Public information can also be seen, accessed, reshared or downloaded through third-party services such as search engines, APIs, and offline media such as TV, and by apps, websites and other services that integrate with our Products.  
  
Learn more about what information is public and how to control your visibility on [Facebook](https://www.facebook.com/help/203805466323736?ref=dp) and [Instagram](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F243810329323104%3Fref%3Ddp&h=AT1MP0_l6mQzn8ZQETgl-_DaC4Unq67UsRmAE0_7jrRGGZz0wOZpM2BXKrLY3HitBylimo6CtaQSF8i3MRwIZkjl51-Tg9sCjw9AL1Nz5mq6ejiu6V_k6uHk2KaaH3I0RvDXNIRZt0_mTrUSnR7d9g).

Content others share or reshare about you

You should consider who you choose to share with, because people who can see your activity on our Products can choose to share it with others on and off our Products, including people and businesses outside the audience you shared with. For example, when you share a post or send a message to specific friends or accounts, they can download, screenshot, or reshare that content to others across or off our Products, in person or in virtual reality experiences such as [Facebook Spaces](https://www.facebook.com/help/241256606347754?ref=dp). Also, when you comment on someone else's post or react to their content, your comment or reaction is visible to anyone who can see the other person's content, and that person can change the audience later.  
  
People can also use our Products to create and share content about you with the audience they choose. For example, people can share a photo of you in a Story, mention or tag you at a location in a post, or share information about you in their posts or messages. If you are uncomfortable with what others have shared about you on our Products, you can learn how to [report the content](https://www.facebook.com/help/181495968648557?ref=dp).

Information about your active status or presence on our Products.

People in your networks can see signals telling them whether you are active on our Products, including whether you are currently active on [Instagram](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F906123729538696%3Fref%3Ddp&h=AT06aQbAEwMo0zP-nFK5U5DmUYxEHEKIscez4WdWQr2mip_tMEgzczmO8QztuCFfRS1JSIQJmFFozT0_oyL5eQf_cMSRpgc1TBkhr41PiMmWs2wTjGD2QPM6l6o04D8V9oO9jW3MalL5oTGPwLmxdA), [Messenger](https://www.facebook.com/help/149081061827062?ref=dp) or Facebook, or when you last used our Products.

Apps, websites, and third-party integrations on or using our Products.

When you choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what you post or share. For example, when you play a game with your Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about your activities in the game or receive a comment or link that you share from the website on Facebook. Also, when you download or use such third-party services, they can access your [public profile](https://www.facebook.com/help/203805466323736?ref=dp) on Facebook, and any information that you share with them. Apps and websites you use may receive your list of Facebook friends if you choose to share it with them. But apps and websites you use will not be able to receive any other information about your Facebook friends from you, or information about any of your Instagram followers (although your friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies, not this one.  
  
Devices and operating systems providing native versions of Facebook and Instagram (i.e. where we have not developed our own first-party apps) will have access to all information you choose to share with them, including information your friends share with you, so they can provide our core functionality to you.  
  
*Note: We are in the process of restricting developers’ data access even further to help prevent abuse. For example, we will remove developers' access to your Facebook and Instagram data if you haven't used their app in 3 months, and we are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, Instagram username and bio, profile photo and email address. Requesting any other data will require our approval.*

New owner.

If the ownership or control of all or part of our Products or their assets changes, we may transfer your information to the new owner.

Sharing with Third-Party Partners

We work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world. We don't sell any of your information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide. Here are the types of third parties we share information with:

Partners who use our analytics services.

We provide aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Pages, videos and other content on and off the Facebook Products. For example, Page admins and Instagram business profiles receive information about the number of people or accounts who viewed, reacted to, or commented on their posts, as well as aggregate demographic and other information that helps them understand interactions with their Page or account.

Advertisers.

We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led you to make a purchase or take an action with an advertiser.

Measurement partners.

We share information about you with companies that aggregate it to provide analytics and measurement reports to our partners.

Partners offering goods and services in our Products.

When you subscribe to receive premium content, or buy something from a seller in our Products, the content creator or seller can receive your public information and other information you share with them, as well as the information needed to complete the transaction, including shipping and contact details.

Vendors and service providers.

We provide information and content to vendors and service providers who support our business, such as by providing technical infrastructure services, analyzing how our Products are used, providing customer service, facilitating payments or conducting surveys.

Researchers and academics.

We also provide information and content to research partners and [academics](https://l.facebook.com/l.php?u=https%3A%2F%2Fresearch.fb.com%2Fprograms%2F&h=AT2dE-XU3POpODb6FhuT-ORXcFvu97I2KDIOlsKKvDAbOcGjT5am8xClaOxBPzD60trs4LJlBTlLpugJwlhdUr-VIf5yCsAO8ao-HDSeRE1sdomIAJ1rS_Nx1PFLPkfApJwFDrtXq-zHMeNUaULWVA) to conduct research that advances scholarship and innovation that support our business or mission, and enhances discovery and innovation on topics of general social welfare, technological advancement, public interest, health and well-being.

Law enforcement or legal requests.

We share information with law enforcement or in response to legal requests in the circumstances outlined [below](https://www.facebook.com/about/privacy/#legal-requests-prevent-harm).

Learn more about how you can control the information about you that you or others share with third-party partners in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT2tfCOvQ0BXkOCEHJekpW8awlbo01bAjS-38xwAcHW8MA464grCH6qkaUKx5DRqV_EmZ6-M8co-vulMUS1EDfXzU_GuKsyuvaKWPhg7tf7YCFGtJ-6Rotzm5YvLm4sAOeMp2GVZUQZBcTxr3P6VmQ).

**How do the Facebook Companies work together?**

Facebook and Instagram share infrastructure, systems and technology with other [Facebook Companies](https://www.facebook.com/help/111814505650678?ref=dp) (which include WhatsApp and Oculus) to provide an innovative, relevant, consistent and safe experience across all [Facebook Company Products](https://www.facebook.com/help/195227921252400?ref=dp) you use. We also process information about you across the Facebook Companies for these purposes, as permitted by applicable law and in accordance with their terms and policies. For example, we process information from WhatsApp about accounts sending spam on its service so we can take appropriate action against those accounts on Facebook, Instagram or Messenger. We also work to understand how people use and interact with Facebook Company Products, such as understanding the number of unique users on different Facebook Company Products.

**What is our legal basis for processing data?**

We [collect](https://www.facebook.com/about/privacy/#collect-information), [use](https://www.facebook.com/about/privacy/#how-we-use-information) and [share](https://www.facebook.com/about/privacy/#information-shared) the data that we have in the ways described above:

* as necessary to fulfill our [Facebook Terms of Service](https://www.facebook.com/legal/terms/update) or [Instagram Terms of Use](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F581066165581870%3Fref%3Ddp&h=AT2Whs3JV4mtWNW0ku-205nemcjNy9aMc4lmxGGXEoeRA8Mil53Q5p1-lWgo_ikjblz13YGMCnDmZIG64cPbQuGM2LTkgdyfDWfpF66mdXkSXngkiP-GqhaTEWhGOzliQDcHhoBllc8642pprgIetQ);
* consistent with your consent, which you may revoke at any time through the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT3nnDRnrxlE6SfVgPAUaEcOb4PiD9s7vxsaLestjm0defZwQckOCUDj4C6Zw1RKMhnXIAQ1KJXCrFFeUBGQ2bdXdj5TIG1LZYhQCF4xF6sgRA96FanQwfqmewqnqzHzVnBLG_iIYRJkpAx92PVUww);
* as necessary to comply with our legal obligations;
* to protect your vital interests, or those of others;
* as necessary in the public interest; and
* as necessary for our (or others') legitimate interests, including our interests in providing an innovative, personalized, safe, and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data.

[Learn more](https://www.facebook.com/about/privacy/legal_bases) about these legal bases and how they relate to the ways in which we process data.

**How can you exercise your rights provided under the GDPR?**

Under the General Data Protection Regulation, you have the right to access, rectify, port and [erase](https://www.facebook.com/help/contact/259518714718624) your data. Learn more about these rights, and find out how you can exercise your rights in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT0tKQu55eN-TOG84vZoj75K7ZVH5vRsiPxGiDYIKbBHpkUWaUzFU_JMtsxGmsO2igTjQoPfkE4HD9hs4cakCuruX9oAi8z2J8ol8EvVA9wUqAhS3o3bP85RgWOltdDX1W5wB-COxkre6O-iZr941Q). You also have the [right to object to](https://www.facebook.com/help/contact/1994830130782319) and restrict certain processing of your data. This includes:

* the right to object to our processing of your data for direct marketing, which you can exercise by using the "unsubscribe" link in such marketing communications; and
* the right to object to our processing of your data where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party. You can exercise this right on Facebook and on Instagram.

**Data retention, account deactivation and deletion**

We store data until it is no longer necessary to provide our services and Facebook Products, or until your account is deleted - whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months. If you submit a copy of your government-issued ID for account verification purposes, we delete that copy 30 days after review, unless otherwise stated. Learn more about deletion of [content you have shared](https://www.facebook.com/help/356107851084108?ref=dp) and [cookie data obtained through social plugins](https://www.facebook.com/help/206635839404055?ref=dp).  
  
When you delete your account, we [delete things](https://www.facebook.com/help/356107851084108?ref=dp) you have posted, such as your photos and status updates, and you won't be able to recover that information later. Information that others have shared about you isn't part of your account and won't be deleted. If you don't want to delete your account but want to temporarily stop using the Products, you can deactivate your account instead. To delete your account at any time, please visit the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Faccounts%2Fprivacy_and_security%2F&h=AT3II0nodf1eG5D2Lx6FNZEms4WJDepdhSVNps8D4e2V1AzUG7I8sLJod8rPwa0Bnk-7bEOzBAsB_xE4QvHsiiE9gpmY5t5awstOIqPslX64X0jRhWfsfeMfHP9Pjzqx2OXYapu50C1WDO1KShEYKA).

**How do we respond to legal requests or prevent harm?**

We access, preserve and share your information with regulators, law enforcement or others:

* In response to a legal request, if we have a good-faith belief that the law requires us to do so. We can also respond to legal requests when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
* When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, we provide information to and receive information from third-party partners about the reliability of your account to prevent fraud, abuse and other harmful activity on and off our Products.

Information we receive about you (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

**How do we operate and transfer data as part of our global services?**

We share information globally, both internally within the Facebook Companies and externally with our partners and with those you connect and share with around the world in accordance with this policy. Information controlled by Facebook Ireland will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes as described in this policy. These data transfers are necessary to provide the services set forth in the [Facebook Terms](https://www.facebook.com/legal/terms/) and [Instagram Terms](https://l.facebook.com/l.php?u=https%3A%2F%2Fhelp.instagram.com%2F581066165581870%3Fref%3Ddp&h=AT1jZFQlRrbFb-8mt7c6h4y1Bh8qQZ5iYLn0hpZT24U_rm5tAmfwlqBtKf7Vh3Lsp-uDWpCWn23XsbFAiCdxR324vdOxXFcPcaN239XyeabGkm19DlpSh6ZogJ5ln44eu-gfPpdskuuqwf2V8YmjTw) and to globally operate and provide our Products to you. We utilize [standard contractual clauses](https://www.facebook.com/help/566994660333381?ref=dp) approved by the European Commission and rely on the European Commission's [adequacy decisions](https://l.facebook.com/l.php?u=https%3A%2F%2Fec.europa.eu%2Finfo%2Flaw%2Flaw-topic%2Fdata-protection%2Fdata-transfers-outside-eu%2Fadequacy-protection-personal-data-non-eu-countries_en&h=AT3tB2ZNS4v8ZNt4Or3R26OP6t4sA9XrK9ub9Pv8Z3iD8e7OvrHGBNSKkWz9snWCcApIVZW9nFwUlvuwBxvrfPy1AXb7xvTG3WkJJpMdgkOI0vclDs8gLHdPjT_YIK1gygP4hUii4884EN1voVAt_A) about certain countries, as applicable, for data transfers from the EEA to the United States and other countries.

**How will we notify you of changes to this policy?**

We'll notify you before we make changes to this policy and give you the opportunity to review the revised policy before you choose to continue using our Products.

Instagram

Data Policy

This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook ([Facebook Products](https://www.facebook.com/help/1561485474074139?ref=dp) or Products). You can find additional tools and information in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/).

**I. What kinds of information do we collect?**

To provide the Facebook Products, we must process information about you. The types of information we collect depend on how you use our Products. You can learn how to access and delete information we collect by visiting the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/).

**Things you and others do and provide.**

* **Information and content you provide.** We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our [camera](https://www.facebook.com/help/162347444215311), so we can do things like suggest masks and filters that you might like, or give you tips on using portrait mode. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described [below](https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc%5b0%5d=Instagram%20Help&bc%5b1%5d=Privacy%20and%20Safety%20Center#how-we-use-information). Learn more about how you can control who can see the things you [share](https://www.facebook.com/help/1297502253597210?ref=dp).
  + Data with special protections: You can choose to provide information in your Facebook [profile fields](https://www.facebook.com/help/353111348061173?ref=dp) or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) is subject to special protections under EU law.
* **Networks and connections.** We collect information about the people, [Pages](https://www.facebook.com/help/282489752085908?ref=dp), accounts, [hashtags](https://help.instagram.com/351460621611097?ref=dp) and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you [choose to upload, sync or import it from a device](https://www.facebook.com/help/561688620598358?ref=dp) (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed [below](https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc%5b0%5d=Instagram%20Help&bc%5b1%5d=Privacy%20and%20Safety%20Center).
* **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.
* **Information about transactions made on our Products.** If you use our Products for [purchases](https://www.facebook.com/help/1434403039959381?ref=dp) or other financial transactions (such as when you make a purchase in a game or make a [donation](https://donations.fb.com/)), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
* **Things others do and information they provide about you.** We also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.

**Device Information**

As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including [ads](https://www.facebook.com/help/119468292028768?ref=dp)) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.

Information we obtain from these devices includes:

* **Device attributes:** information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
* **Device operations:** information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
* **Identifiers:** unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to [Facebook Company Products](https://www.facebook.com/help/195227921252400?ref=dp) associated with the same device or account).
* **Device signals:** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
* **Data from device settings:** information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
* **Network and connections:** information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you [stream a video from your phone to your TV](https://www.facebook.com/help/276515126152168?ref=dp).
* **Cookie data:** data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the [Facebook Cookies Policy](https://www.facebook.com/policies/cookies/) and [Instagram Cookies Policy](https://www.instagram.com/legal/cookies/).

**Information from partners.**

Advertisers, [app](https://www.facebook.com/help/1642635852727373?ref=dp) developers, and publishers can send us information through [Facebook Business Tools](https://www.facebook.com/help/331509497253087) they use, including our social plug-ins (such as the Like button), Facebook Login, our [APIs and SDKs](https://developers.facebook.com/docs/apis-and-sdks), or the Facebook [pixel](https://www.facebook.com/business/a/facebook-pixel). These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. [Learn more](https://www.facebook.com/help/494750870625830?ref=dp) about the types of partners we receive data from.

To learn more about how we use cookies in connection with Facebook Business Tools, review the [Facebook Cookies Policy](https://www.facebook.com/policies/cookies) and [Instagram Cookies Policy](https://www.instagram.com/legal/cookies/).

**II. How do we use this information?**

We use the information we have (subject to choices you make) as described below and to provide and support the Facebook Products and related services described in the [Facebook Terms](https://www.facebook.com/legal/terms/update) and [Instagram Terms](https://help.instagram.com/581066165581870?ref=dp). Here's how:

**Provide, personalize and improve our Products.**

We use the information we have to deliver our Products, including to personalize features and content (including your [News Feed](https://www.facebook.com/help/166738576721085?ref=dp), [Instagram Feed](https://help.instagram.com/1986234648360433?ref=dp), Instagram Stories and ads) and make suggestions for you (such as groups or [events](https://www.facebook.com/help/1076296042409786?ref=dp) you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any [data with special protections](https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc%5b0%5d=Instagram%20Help&bc%5b1%5d=Privacy%20and%20Safety%20Center#data-special-protections) you choose to provide where you have given your explicit consent); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products. Learn more about how we use information about you to personalize your Facebook and Instagram experience, including features, content and recommendations in Facebook Products; you can also learn more about how we choose the [ads](https://www.facebook.com/about/ads) that you see.

* **Information across Facebook Products and devices:** We connect information about your activities on different Facebook Products and devices to provide a more tailored and consistent experience on all Facebook Products you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger. We can also make your experience more seamless, for example, by automatically filling in your registration information (such as your phone number) from one Facebook Product when you sign up for an account on a different Product.
* **Location-related information:** We use [location-related information](https://www.facebook.com/about/basics/manage-your-privacy/location)-such as your current location, where you live, the places you like to go, and the businesses and people you're near-to provide, personalize and improve our Products, [including ads](https://www.facebook.com/about/ads), for you and others. Location-related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Facebook Products (such as check-ins or events you attend).
* **Product research and development:** We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.
* **Face recognition:** If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create are [data with special protections](https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc%5b0%5d=Instagram%20Help&bc%5b1%5d=Privacy%20and%20Safety%20Center#data-special-protections) under EU law. Learn more about [how we use face recognition technology](https://www.facebook.com/help/122175507864081?ref=dp), or control our use of this technology in [Facebook Settings](https://www.facebook.com/settings/facerec). If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.
* **Ads and other sponsored content:** We use the information we have about you-including information about your interests, actions and connections-to select and personalize ads, offers and other sponsored content that we show you. Learn more about how we [select and personalize ads](https://www.facebook.com/ads/preferences), and your choices over the data we use to select ads and other sponsored content for you in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/).

**Provide measurement, analytics, and other business services.**

We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services. [Learn how we share information](https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc%5b0%5d=Instagram%20Help&bc%5b1%5d=Privacy%20and%20Safety%20Center#sharing-partner-information) with these partners.

**Promote safety, integrity and security.**

We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to [detect when someone needs help](https://code.facebook.com/posts/286893341840510/under-the-hood-suicide-prevention-tools-powered-by-ai/). To learn more, visit the [Facebook Security Help Center](https://www.facebook.com/help/379220725465972?ref=dp) and [Instagram Security Tips](https://help.instagram.com/369001149843369).

**Communicate with you.**

We use the information we have to send you marketing communications, communicate with you about our Products, and let you know about our policies and terms. We also use your information to respond to you when you contact us.

**Research and innovate for social good.**

We use the information we have (including from research partners we collaborate with) to conduct and support [research](https://research.fb.com/) and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. For example, [we analyze information we have about migration patterns during crises](https://research.fb.com/facebook-disaster-maps-methodology/) to aid relief efforts. [Learn more](https://research.fb.com/) about our research programs.

**III. How is this information shared?**

Your information is shared with others in the following ways:

**Sharing on Facebook Products**

**People and accounts you share and communicate with**

When you share and communicate using our Products, [you choose the audience for what you share](https://www.facebook.com/help/120939471321735?ref=dp). For example, when you post on Facebook, you select the audience for the post, such as a group, all of your friends, the public, or a customized list of people. Similarly, when you use Messenger or Instagram to communicate with people or businesses, those people and businesses can see the content you send. Your network can also see actions you have taken on our Products, including engagement with ads and sponsored content. We also let other accounts see who has viewed their Facebook or Instagram Stories.

[**Public information**](https://www.facebook.com/help/203805466323736?ref=dp) can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your [public profile on Facebook](https://www.facebook.com/help/203805466323736?ref=dp); and content you share on a Facebook Page, [public Instagram account](https://help.instagram.com/448523408565555?ref=dp) or any other public forum, such as [Facebook Marketplace](https://www.facebook.com/marketplace). You, other people using Facebook and Instagram, and we can provide access to or send public information to anyone on or off our Products, including in other Facebook Company Products, in search results, or through tools and APIs. Public information can also be seen, accessed, reshared or downloaded through third-party services such as search engines, APIs, and offline media such as TV, and by apps, websites and other services that integrate with our Products.

Learn more about what information is public and how to control your visibility on [Facebook](https://www.facebook.com/help/203805466323736?ref=dp) and [Instagram](https://help.instagram.com/243810329323104?ref=dp).

**Content others share or reshare about you**

You should consider who you choose to share with, because people who can see your activity on our Products can choose to share it with others on and off our Products, including people and businesses outside the audience you shared with. For example, when you share a post or send a message to specific friends or accounts, they can download, screenshot, or reshare that content to others across or off our Products, in person or in virtual reality experiences such as [Facebook Spaces](https://www.facebook.com/help/241256606347754?ref=dp). Also, when you comment on someone else's post or react to their content, your comment or reaction is visible to anyone who can see the other person's content, and that person can change the audience later.

People can also use our Products to create and share content about you with the audience they choose. For example, people can share a photo of you in a Story, mention or tag you at a location in a post, or share information about you in their posts or messages. If you are uncomfortable with what others have shared about you on our Products, you can learn how to [report the content](https://www.facebook.com/help/181495968648557?ref=dp).

**Information about your active status or presence on our Products.**

People in your networks can see signals telling them whether you are active on our Products, including whether you are currently active on [Instagram](https://help.instagram.com/906123729538696?ref=dp), [Messenger](https://www.facebook.com/help/149081061827062?ref=dp) or Facebook, or when you last used our Products.

**Apps, websites, and third-party integrations on or using our Products.**

When you choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what you post or share. For example, when you play a game with your Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about your activities in the game or receive a comment or link that you share from the website on Facebook. Also, when you download or use such third-party services, they can access your public profile on Facebook, and any information that you share with them. Apps and websites you use may receive your list of Facebook friends if you choose to share it with them. But apps and websites you use will not be able to receive any other information about your Facebook friends from you, or information about any of your Instagram followers (although your friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies, not this one.

Devices and operating systems providing native versions of Facebook and Instagram (i.e. where we have not developed our own first-party apps) will have access to all information you choose to share with them, including information your friends share with you, so they can provide our core functionality to you.

*Note: We are in the process of restricting developers’ data access even further to help prevent abuse. For example, we will remove developers' access to your Facebook and Instagram data if you haven't used their app in 3 months, and we are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, Instagram username and bio, profile photo and email address. Requesting any other data will require our approval.*

**New owner.**

If the ownership or control of all or part of our Products or their assets changes, we may transfer your information to the new owner.

**Sharing with Third-Party Partners**

We work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world. We don't sell any of your information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide. Here are the types of third parties we share information with:

**Partners who use our analytics services.**

We provide aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Pages, videos and other content on and off the Facebook Products. For example, Page admins and Instagram business profiles receive information about the number of people or accounts who viewed, reacted to, or commented on their posts, as well as aggregate demographic and other information that helps them understand interactions with their Page or account.

**Advertisers.**

We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led you to make a purchase or take an action with an advertiser.

**Measurement partners.**

We share information about you with companies that aggregate it to provide analytics and measurement reports to our partners.

**Partners offering goods and services in our Products.**

When you subscribe to receive premium content, or buy something from a seller in our Products, the content creator or seller can receive your public information and other information you share with them, as well as the information needed to complete the transaction, including shipping and contact details.

**Vendors and service providers.**

We provide information and content to vendors and service providers who support our business, such as by providing technical infrastructure services, analyzing how our Products are used, providing customer service, facilitating payments or conducting surveys.

**Researchers and academics.**

We also provide information and content to research partners and [academics](https://research.fb.com/programs/) to conduct research that advances scholarship and innovation that support our business or mission, and enhances discovery and innovation on topics of general social welfare, technological advancement, public interest, health and well-being.

**Law enforcement or legal requests.**

We share information with law enforcement or in response to legal requests in the circumstances outlined below.

Learn more about how you can control the information about you that you or others share with third-party partners in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/).

**IV. How do the Facebook Companies work together?**

Facebook and Instagram share infrastructure, systems and technology with other [Facebook Companies](https://www.facebook.com/help/111814505650678?ref=dp) (which include WhatsApp and Oculus) to provide an innovative, relevant, consistent and safe experience across all [Facebook Company Products](https://www.facebook.com/help/195227921252400ref=dp) you use. We also process information about you across the Facebook Companies for these purposes, as permitted by applicable law and in accordance with their terms and policies. For example, we process information from WhatsApp about accounts sending spam on its service so we can take appropriate action against those accounts on Facebook, Instagram or Messenger. We also work to understand how people use and interact with Facebook Company Products, such as understanding the number of unique users on different Facebook Company Products.

**V. What is our legal basis for processing data?**

We collect, use and share the data that we have in the ways described above:

* as necessary to fulfill our [Facebook Terms of Service](https://www.facebook.com/legal/terms/update) or [Instagram Terms of Use](https://help.instagram.com/581066165581870?ref=dp);
* consistent with your consent, which you may revoke at any time through the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/);
* as necessary to comply with our legal obligations
* to protect your vital interests, or those of others;
* as necessary in the public interest; and
* as necessary for our (or others') legitimate interests, including our interests in providing an innovative, personalized, safe, and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data.

[Learn more](https://www.facebook.com/about/privacy/legal_bases) about these legal bases and how they relate to the ways in which we process data.

**VI. How can you exercise your rights provided under the GDPR?**

Under the General Data Protection Regulation, you have the right to access, rectify, port and [erase](https://help.instagram.com/contact/448642219041658) your data. Learn more about these rights, and find out how you can exercise your rights in the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/). You also have the [right to object to](https://help.instagram.com/contact/1845713985721890) and restrict certain processing of your data. This includes:

* the right to object to our processing of your data for direct marketing, which you can exercise by using the "unsubscribe" link in such marketing communications; and
* the right to object to our processing of your data where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party. You can exercise this right on Facebook and on Instagram.

**VII. Data retention, account deactivation and deletion**

We store data until it is no longer necessary to provide our services and Facebook Products, or until your account is deleted - whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months. If you submit a copy of your government-issued ID for account verification purposes, we delete that copy 30 days after review, unless otherwise stated. Learn more about deletion of [content you have shared](https://www.facebook.com/help/356107851084108?ref=dp) and [cookie data obtained through social plugins](https://www.facebook.com/help/206635839404055?ref=dp).

When you delete your account, we [delete things](https://www.facebook.com/help/356107851084108?ref=dp) you have posted, such as your photos and status updates, and you won't be able to recover that information later. Information that others have shared about you isn't part of your account and won't be deleted. If you don't want to delete your account but want to temporarily stop using the Products, you can deactivate your account instead. To delete your account at any time, please visit the [Facebook Settings](https://www.facebook.com/settings) and [Instagram Settings](https://www.instagram.com/accounts/privacy_and_security/).

**VIII. How do we respond to legal requests or prevent harm?**

We access, preserve and share your information with regulators, law enforcement or others:

* In response to a legal request, if we have a good-faith belief that the law requires us to do so. We can also respond to legal requests when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
* When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, we provide information to and receive information from third-party partners about the reliability of your account to prevent fraud, abuse and other harmful activity on and off our Products.

Information we receive about you (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

**IX. How do we operate and transfer data as part of our global services?**

We share information globally, both internally within the Facebook Companies and externally with our partners and with those you connect and share with around the world in accordance with this policy. Information controlled by Facebook Ireland will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes as described in this policy. These data transfers are necessary to provide the services set forth in the [Facebook Terms](https://www.facebook.com/legal/terms/) and [Instagram Terms](https://help.instagram.com/581066165581870?ref=dp) and to globally operate and provide our Products to you. We utilize [standard contractual clauses](https://www.facebook.com/help/566994660333381?ref=dp) approved by the European Commission and rely on the European Commission's [adequacy decisions](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en) about certain countries, as applicable, for data transfers from the EEA to the United States and other countries.

**X. How will we notify you of changes to this policy?**

We'll notify you before we make changes to this policy and give you the opportunity to review the revised policy before you choose to continue using our Products.

**XI. How to contact Facebook with questions**

You can learn more about how privacy works [on Facebook](https://www.facebook.com/about/basics) and on [Instagram](https://help.instagram.com/196883487377501?ref=dp). If you have questions about this policy, you can contact us as described below.

The data controller responsible for your information is Facebook Ireland, which you can [contact online](https://help.instagram.com/contact/186020218683230), or by mail at:  
  
Facebook Ireland Ltd.  
4 Grand Canal Square  
Grand Canal Harbour  
Dublin 2 Ireland  
  
[Contact the Data Protection Officer for Facebook Ireland Ltd.](https://www.facebook.com/help/contact/540977946302970)  
  
You also have the right to lodge a complaint with Facebook Ireland's lead supervisory authority, the Irish Data Protection Commissioner, or your local supervisory authority

Protonmail

Privacy Policy

In the following policy, ProtonMail refers to the service offered by Proton Technologies AG (the "Company" or "We") through the protonmail.com website (the "Service"). This Privacy Policy explains (i) what information we collect through your access and use of our Service (ii) the use we make of such information; and (iii) the security level we provide for protecting such information.

By visiting protonmail.com and using the Services provided here, you agree to the terms outlined in this privacy policy.

Legal Framework

The Company is domiciled in Switzerland at the following address:

Proton Technologies AG, Route de la Galaise 32, 1228 Plan-les-Ouates Geneva, Switzerland

All data storage infrastructure is also located solely within Switzerland, and thus governed by the laws and regulations of Switzerland. Additional information about the legal framework can be found in our [Transparency Report](https://protonmail.com/blog/transparency-report/).

Data related to the opening of an account

Any email address provided to ProtonMail through either our waiting list, optional email verification, or optional notification/recovery email setting in your account, is considered personal data as defined and protected by the Swiss Federal Data Protection Act (DPA).

Such data will only be used to contact you with important notifications about ProtonMail, to send you information related to security, to send you an invitation link to create your ProtonMail account, to verify your ProtonMail account, or to send you password recovery links if you enable the option. We may also inform you about new Proton products in which you might have an interest. You are free, at any given time, to opt-out of those features through the account settings panel.

In order to maintain the integrity of the service, ProtonMail must take measures to avoid creation of accounts by spammers. This is because if spammers use ProtonMail to send messages, ProtonMail’s IP addresses can become blocked by major mail providers such as Gmail, Yahoo, Outlook, etc.

In order to pursue our legitimate interest of preventing the creation of accounts by spam bots or human spammers, ProtonMail uses a variety of human verification methods. You may be asked to verify using either reCaptcha, Email, or SMS. IP addresses, email addresses, and phone numbers provided are saved temporarily in order to send you a verification code and to determine if you are a spammer. If this data is saved permanently, it is always saved as a cryptographic hash, which ensures that the raw values cannot be deciphered by us. [Learn More](https://protonmail.com/support/knowledge-base/human-verification/)

Data Collection

Our company’s overriding policy is to collect as little user information as possible to ensure a completely private and anonymous user experience when using the Service. We also have no technical means to access your encrypted message contents.

Service's user data collection is limited to the following:

**Visiting our website:** We employ a local installation of Matomo, an open source analytics tool. Analytics are anonymized whenever possible and stored locally (and not on the cloud).

**Account creation:** It is not necessary to provide personal information in order to create an account, but you may provide an external email address for notification or password recovery purposes. Should you choose to provide it, we do associate another email address with your account (for password recovery, or notifications). The legal basis for processing is consent and you are free to remove that data in the account panel of your ProtonMail account.

**Account activity:** Due to limitations of the SMTP protocol, we have access to the following email metadata: sender and recipient email addresses, the IP address incoming messages originated from, message subject, and message sent and received times. We do NOT have access to encrypted message content but unencrypted messages sent from external providers to ProtonMail are scanned for Spam and Viruses to pursue the legitimate interest of the protection of our users. We also have access to the following records of account activity: number of messages sent, amount of storage space used, total number of messages, last login time.

**Communicating with ProtonMail:** Your communications with the Company, such as support requests, bug reports, or feature requests may be saved by our staff. The legal basis for processing is our legitimate interest to troubleshoot more efficiently and improve the quality of the ProtonMail service.

**IP Logging:** By default, ProtonMail does not keep permanent IP logs. However, IP logs may be kept temporarily to combat abuse and fraud, and your IP address may be retained permanently if you are engaged in activities that breach our terms and conditions (spamming, DDoS attacks against ProtonMail infrastructure, brute force attacks, etc). The legal basis of this processing is our legitimate interest to protect our service against nefarious activities.  
  
Your login IP address is also kept permanently (until you delete it) if you enable authentication logging for your account (by default this is off). The legal basis of this processing is consent, and you are free to opt-in or opt-out at any time in the security panel of your ProtonMail account.

**Payment Information:** The Company relies on third parties to process credit card, PayPal, and Bitcoin transactions so the Company necessarily must share payment information with third parties. Anonymous cash or Bitcoin payments and donations are accepted however. The legal basis of this processing is the necessity to the execution of the contract between you and us.

**Native Applications:** When you use our native applications, we (or the mobile app platform providers) may collect certain information in addition to the information mentioned elsewhere in this Policy. We may use mobile analytics software (such as fabric.io app statistics and crash reporting, Play Store app statistics, App Store app statistics, or self-hosted Sentry crash reporting) to send crash information to our developers so that we can fix bugs rapidly. Some platforms (such as the Google Play Store or the Apple App Store) may also collect aggregate, anonymous statistics like which type of devices and operating systems that are most commonly used (like percentage of Android 6.x vs Android 7.x), the total number of installs, total number of uninstalls, and the total number of active users, and may be governed by the privacy policy and terms and conditions of the Google Play Store or the Apple App Store. None of the software on our apps will ever access or track any location-based information from your device at any time. Any personal data acquired during this process is anonymized.

**Import Assistant Tool:** When you use our Import Assistant Tool to import your emails from another service provider, the credentials of the email account from which the importation is performed are stored by the Company for the duration of the importation. Once the importation is performed, those credentials are entirely deleted from our systems.

Data Use

We do not have any advertising on our site. Any data that we do have will never be shared except under the circumstances described below in the Data Disclosure Section. We do NOT do any analysis on the limited data we do possess with two exceptions:

* Emails sent unencrypted to ProtonMail accounts (e.g. Gmail to ProtonMail) are scanned automatically pursuing the legitimate interest of detecting spam so we can block IPs which are sending a lot of spam to ProtonMail users and place spam messages in a spam directory. Inbound messages are scanned for spam in memory, and then encrypted and written to disk. We do not possess the technical ability to scan messages after they have been encrypted.
* Emails sent by ProtonMail users to outside (e.g. Gmail) users with encryption disabled are scanned automatically pursuing the legitimate interest of detecting spam in the same manner as incoming email. This is to ensure a ProtonMail account which is being used for spamming purposes can be detected and locked so email deliverability for legitimate users is not degraded.

Data Storage

All servers used in connection with the provisioning of the Service are located in Switzerland and wholly owned and operated by the Company. Only employees of the Company have physical or other access to the servers. Data is ALWAYS stored in encrypted format on our servers. Offline backups may be stored periodically, but these are also encrypted. We do not possess the ability to access any user encrypted message content on either the production servers or in the backups.

Third Party Networks

Proton's alternative routing technology allows Proton apps to bypass many censorship blocks, but your network traffic may go through third party networks which we do not control. This could enable a third party to record your IP address or see that you are using Proton apps (the same information that your Internet Service Provider is able to see). These third parties cannot see your actual data, which remains encrypted. By default, alternative routing is not used for Proton apps unless they detect that censorship measures are active on your network. Alternative routing can also be completely disabled in the Settings panel of all of our mobile and desktop applications. However, doing so may cause you to be unable to access your Proton account if you are on a network that is censoring Proton. [Learn more](https://protonmail.com/blog/anti-censorship-alternative-routing)

Right to Access, Rectification, Erasure, Portability, and right to lodge a complaint

Through the Service, you can directly access, edit, delete or export personal data processed by the Company in your use of the Service.

If your account has been suspended for a breach of our terms and conditions, and you would like to exercise the rights related to your personal data, you can make a request to our support team.

In case of violation of your rights, you have the right to lodge a complaint to the competent supervisory authority.

Data Retention

When a ProtonMail account is closed, data is immediately deleted from production servers. Active accounts will have data retained indefinitely. Deleted emails are also permanently deleted from production servers. Deleted data may be retained in our backups for up to 14 days.

Data Disclosure

We will only disclose the limited user data we possess if we are instructed to do so by a fully binding request coming from the competent Swiss authorities (legal obligation). While we may comply with electronically delivered notices (see exceptions below), the disclosed data can only be used in court after we have received an original copy of the court order by registered post or in person, and provide a formal response.

If a request is made for encrypted message content that ProtonMail does not possess the ability to decrypt, the fully encrypted message content may be turned over. If permitted by law, ProtonMail will always contact a user first before any data disclosure. Under Swiss law, it is obligatory to notify the target of a data request, although such notification may come from the authorities and not from the Company.

ProtonMail may from time to time, contest requests if there is a public interest in doing so. In such situations, the Company will not comply with the request until all legal or other remedies have been exhausted. Therefore, not all requests described in our Transparency Report will lead to data disclosure.

Modifications to Privacy Policy

ProtonMail reserves the right to periodically review and change this policy from time to time and we will notify users who have enabled the notificationn preference about changes to our Privacy Policy. Continued use of the Service will be deemed as acceptance of such changes.

Norton Lifelock

1. [Privacy](https://www.nortonlifelock.com/us/en/privacy/)

When it comes to your personal data, NortonLifeLock, including Norton which is a division of NortonLifeLock, and LifeLock, Inc., which is a wholly owned subsidiary of NortonLifeLock (collectively referred to as “NortonLifeLock”, “Norton”, “LifeLock”, “we” or “us”), as well as our employees, contractors and service providers, are committed to providing you with transparency and choice. We process personal data in accordance with applicable legislation, while taking into account and balancing the relevant interests of our customers, ourselves and other stakeholders.

We do not, and will not without consent, sell, lease, or rent your information to third parties for monetary or other valuable consideration.

This Privacy Statement (“Statement”) provides an overview of how we, via our websites, products and services (“Services”), process and protect your personal data. This Statement applies to the NortonLifeLock websites, products and services that link to or reference this Statement and describes how we collect, process and share personal data and the choices available to you regarding collection and use of your personal data. Additional information on our personal data practices may be provided in offer descriptions, contractual terms, supplemental privacy statements, or notices provided prior to or at the time of data collection. In addition, we provide Product and Service Privacy Notices describing in more detail the collection and processing of personal data through your use of such products and services, and those can be found at [nortonlifelock.com/privacy](https://www.nortonlifelock.com/privacy/). If any other privacy notice conflicts with this Privacy Statement, such specific notice will take precedence.

If you are in the European Economic Area, and unless stipulated otherwise contractually, the Controller of your personal data is NortonLifeLock Ireland Limited, which has its principal place of business at Ballycoolin Business Park, Blanchardstown, Dublin 15, Ireland.

You need not enroll or register with us to just visit and view our Site. However, if you elect to obtain or use any of our products or services you must register or enroll (or be enrolled by an authorized third-party) with us, and you must agree to the applicable customer agreement, product end-user license agreements or service terms.

What this Statement Covers:

**1) Personal Data Collection and Handling Practices**

* How we collect personal data, and from what sources;
* The categories of personal data we collect;
* The purpose for which we collect and process that personal data;
* When and why we share your personal data with third-parties, and the types of third-parties with which we may share personal data;
* Retention and deletion of your personal data;
* Cross border transfers of personal data; and
* How we protect your personal data.

**2) Your Privacy Rights**

* Your Privacy Rights; and
* How to contact us about privacy matters.

**3) Referrals, Marketing, Opt-In/Opt-Out, and Cookies**

* Referrals;
* Marketing and community networking;
* How to opt out of Internet-based advertising;
* Cookies and tracking technologies; and
* Automated individual decision making and profiling.

**4) Children’s Privacy**

**5) Miscellaneous**

* Changes to this Statement;
* Links to Other Websites.

Personal Data Collection and Handling Practices

How we collect your personal data and from what Sources

**We collect personal data in the following ways from the following sources:**

1) Automatically from your visits to our Sites or use of our products/services;

2) From you when you interact with our agents through calls and chat sessions and provide personal data to us (either about yourself or a third-party (e.g. customer or employment referral));

3) From third-parties (e.g. marketing leads) and public sources, subject to applicable laws and regulations.

**Method and Sources of Collection:**

We may collect personal data about you from the following sources:

* From You:
  + When you visit and use our websites, products and services, we automatically may collect data about your use of our websites, products and services;
  + When you interact directly with us, we may collect personal data that you provide to us (e.g. account and payment information);
* Third-Parties:
  + We may collect personal data about you from third-parties such as:
    - credit reporting agencies and financial institutions (used for purposes such as identity theft protection services),
    - marketing and joint-marketing partners (used for purposes such as to offer products/services and/or joint product bundles to prospective members),
    - public sources (such as The Dark Web to alert you to potential misuse of your data, and Data Broker sites allowing you to remove your data at your discretion, and other sources for purposes such as to identify prospective customers or alert customers to potential fraud).

We may collect personal data *from you about other people*, such as personal data about friends and family through customer or employee referrals, or data about family members who you wish to include on your account.

Additional detail on the use of your personal data can be found in the “Purposes of Processing” section below.

Categories of personal data we Collect and General Purpose of Collection

**We collect the following categories of personal data for the following general purposes:**

1) **Member/Subscriber Information** is collected to manage our business relationship with you;

2) **Administrative Data** is data collected to maintain our business records;

3) **Provisioning Data** is collected to deliver our products and services;

4) **Security Data** is collected to provide Cyber Safety services, and to prevent fraud and identity theft;

5) **Diagnostic Information** is collected to troubleshoot malfunctioning products and services;

6) **Usage and Preference Data** is collected to help us provide you with better service and user experience; and

7) **Third-Party Data** provided by you or collected by us is collected as necessary to deliver or promote our services or recruit for potential open employment positions.

**Categories of Personal Data We collect:**

The categories of personal data that we collect, and the general purposes of collection, include:

* **Member/Subscriber Information**. This information includes data necessary to establish your account and method/means of payment, ship your products or provide services, and track and maintain our relationship with you. It includes:
  + Identifiers and contact details, including name, mailing address, email address, phone number and member credentials (user ID and password);
  + Shipping and billing data, including credit card and payment data;
  + Your social security number and/or state/government identifier, driver’s license number or other government-issued identifier, date of birth, age and gender, and other personal details about you as necessary to verify your identity and to provide identity theft protection services; and
  + Commercial information, including your transaction history with us.
* **Administrative Data**. This is data that is generated by us and is related to your account, device or use of services. It includes license keys and internally-created member IDs, and device IDs, and serves the purposes of maintaining our business records and enforcing product license and service entitlement compliance.
* **Provisioning Data**. This includes data necessary to provision applications or to facilitate installation and may include device and system information, browser type, IP address, type of operating system, and internet or other electronic network activity information.
* **Security Data**. This data may include bank transaction data, credit alerts, location data, and data identified below that is collected for cyber threat intelligence, as needed to provide cyber safety and identity theft protection services, as well as to protect against fraud.
* **Diagnostic Information**. This data may include application crash reports and information you provide to us for obtaining customer service, as necessary to troubleshoot any malfunctioning products and services. For example, when you call or exchange email, chat or mail with us, we may retain and review call and chat recordings and/or the contents of the messages as required/permitted by law and our recording and information management policies.
* **Usage and Preference Information**. This information includes data received directly from you, and/or derived from cookies (tags, pixels, etc.) and third-parties indicating usage and preferences, and product/service and communication preferences as set by you. It helps us better understand and better serve your interests, expectations, needs and requirements.
* **Third-Party Data**. This information includes data we may obtain from you about a third-party, or data about a third-party we collect from you and/or through the provision of our services, including threat intelligence data used to analyze threats and protect you, us and our other customers against fraud and cyber threats. Third-Party Data may include email and IP address of the sender of malicious malware.

The Purpose of Processing Your Personal Data

**We may process your personal data:**

1) for the purpose of fulfilling our contract with you (e.g. for the provision of products and services, providing customer service, etc.);

2) for specified purposes on the basis of your consent (e.g. marketing, surveys, etc.);

3) for the purpose of fulfilling our legal obligations (e.g. maintaining employment and tax records, responding to lawful subpoenas, etc.), and;

4) for the purpose of pursing our legitimate business interests, including:

* Conducting Routine Business Activities, such as marketing, product research, providing customized web experiences, etc.;
* Combining Data to Improve our Customers’ Experience and Evaluate/Refine our Products and Services;
* For Network and Information Security Purposes; and,
* For Developing Cyber-threat intelligence data to better understand, anticipate and counter cyber threats.

We collect and process your personal data for the purposes outlined below as well as in the relevant Product and Service Privacy Notices on the following grounds:

**1) For the purpose of fulfilling our contract** with you or entering into a contract with you on your request, in order to:

* Create and manage your account;
* Authenticate you prior to enrolling in services;
* Verify your identity and entitlement to products or services, when you contact us or access our services;
* Process your purchase transactions;
* Update you on the status of your orders;
* Allow you to register products or services your purchase;
* Manage your subscriptions; and
* Provide you with technical and customer support.

**2) For specific purposes based on your consent**, in order to:

* Subscribe you to newsletters, send you product updates or technical alerts;
* Send you marketing communications and information on new products, services and assets;
* Communicate with you about, and manage your participation in contests, offers or promotions;
* Solicit your opinion or feedback, provide opportunities for you to test products or services;
* Enable you to refer a friend who may be interested in our offerings, as permitted by law;
* Where required and applicable, to enable any non-essential cookies or similar technologies;
* Process sensitive personal data in accordance with applicable law, and
* Provide you with interest-based ads on sites other than our own.

**3) For the purpose of fulfilling our legal obligations,** we may be obligated to, for instance, keep and process records for tax purposes or in order to meet legal obligations and disclosures.

**4) For the purpose of promoting and operating our business and advancing our legitimate interests** in the effective delivery of our products, services and communications to you as well as to our other customers and partners. Specifically, in order to:

* Provide you with information, products and services that you request; enable participation in interactive features of our Services; and notify you about changes to our terms or this Privacy Statement;
* Communicate commercial promotions and provide quotes for our products and services;
* Promote and administer co-branded offers with trusted partners;
* Confirm sales conversions and conduct lead generation activities;
* Better administer and understand the usability, performance, and effectiveness of our Services, including troubleshooting, data analytics, testing, research, and statistical purposes;
* Improve our Services (including developing new Services) and to ensure that content is customized and presented in the most relevant and effective manner for you and for your device, including suggestions and recommendations about things that may be of interest to you;
* \*Ensure the security of our own, and of our customers’ networks and information systems, including the development of threat intelligence resources;
* \*Develop cyber-threat intelligence resources; and
* \*Otherwise keep our Services, business and users safe and secure; to comply with applicable laws and regulations; and to protect or exercise our legal rights or defend against legal claims.

**\*For Network and Information Security Purposes and Cyber-threat Intelligence:**

It is in our legitimate interests as well as in our customers’ interests to collect and process personal data to the extent strictly necessary and proportionate **for the purposes of ensuring the security of our own, and of our customers’ networks, information systems, and the identity of the individuals using or otherwise benefitting from them**. This includes the development of threat intelligence resources aimed at maintaining and improving on an ongoing basis the ability of information networks and systems to resist unlawful or malicious actions and other harmful events, such as cybercriminal activities and attempts at identity theft or fraud (“cyber and identity threats”).

The personal data we process for Network and Information Security Purposes includes, without limitation, network traffic data related to cyber and identity threats such as:

* sender email addresses (e.g., of sources of SPAM such as phishing scams);
* recipient email addresses (e.g., of victims of targeted email attacks);
* reply-to email addresses (e.g., as configured by cybercriminals sending malicious email);
* filenames and execution paths (e.g., of malicious or otherwise harmful executable files attached to emails);
* URLs and associated page titles (e.g., of web pages broadcasting or hosting malicious or otherwise harmful contents); and/or
* IP addresses (e.g., of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching or other storage of cyber and identity threats such as malicious or otherwise harmful contents).

Depending on the context in which such data is collected, it may contain personal data concerning you or third-parties. However, in such cases, we will process the data only to the extent strictly necessary and proportionate to the purposes of detecting, blocking, reporting (by removing any personally identifiable elements) and mitigating the cyber or identity threats of concern, or to other users relying on our products and services to protect their networks, systems and identities. When processing personal data in this context, we will only identify specific data subjects if and to the extent necessary for the remediation of the cyber or identity threats concerned, or as required by law.

If you believe that your personal data was unduly collected or is unduly processed by NortonLifeLock for such purposes, please refer to the “Your Rights” and “Contact Us” sections. Please be aware that if it is determined that personal data concerning you is processed by NortonLifeLock because it is necessary for the detection, blocking or mitigation of convicted cyber or identity threats, objection, rectification or erasure requests may be rejected in accordance with applicable law.

When and Why We Share Your Personal Data

We only share your personal data outside the NortonLifeLock organization to such authorized third-parties as our business partners for purposes of promoting or selling our products (alone or jointly with theirs), service providers who perform necessary business services for us under written agreement, the public authorities who may obtain your personal data subject to applicable legal and regulatory authority, or where otherwise required by law. In providing restoration services, we may share your personal data with third-party vendors or financial institutions subject to your knowledge and, where applicable, consent.

We are committed to maintaining your trust, and we want you to understand when and with whom we may share the information we collect. We do not, and will not without consent, sell, lease, or rent your information to third parties for monetary or other valuable consideration.

We do permit third-parties to collect any of the information described above through our Services and disclose information to third-parties for the following business purposes, in which case we require these recipients to comply with adequate privacy and confidentiality requirements and security standards:

**Partners**

We may provide your personal data to our partners for the purpose of allowing them to conduct NortonLifeLock business. Our partners go through our third-party risk management and assessment process and only afterwards are they authorized to promote and sell our products and services. Our partners may use your personal data to communicate with you and others about NortonLifeLock Services either alone or jointly with partner products and services. We may provide your personal data to partners to confirm your eligibility for joint or co-branded offers or to communicate and administer such offers (e.g. report sales conversions, verify eligibility, assess effectiveness of joint offer, etc.) *Our Partners are not allowed to use personal data that they receive from us for any purpose except for communicating, evaluating, improving and administering the offer in question (NortonLifeLock branded, co-branded or joint offer).* This will not affect the partner’s ability to use personal data that it may already have obtained from you or other sources. If you do not wish to receive promotional emails from our partners, you can unsubscribe directly using the unsubscribe link or tool provided in the partner’s email or other communication to you.

**Service Providers Processing Data on Our Behalf**

We may use contractors and service providers to process your personal data on our behalf for the purposes described in this Statement, the relevant product and service privacy notices and for business purposes such as financial auditing, data storage and security, troubleshooting and debugging, improving and operationalizing threat intelligence and counter-threat measures, and for marketing and promoting our Services. We contractually require service providers to keep data confidential and we do not allow our service providers to disclose your personal data to others without our authorization, or to sell it or use it for purposes unrelated to the services they provide (e.g. their own marketing purposes). However, if you have a separate and/or independent relationship with these service providers, their privacy statements will apply to such relationships. Such service providers may include benefit brokers, your employer (for products and services offered as an employee benefit), contact centers, payment card processors and marketing/survey/analytics suppliers.

**Public Authorities**

In certain instances, it may be necessary for us to disclose your personal data to public authorities or as otherwise required by applicable law. No personal data will be disclosed to any public authority except in response to:

* A subpoena, warrant or other legal process issued by a court or other public authority of competent jurisdiction;
* A legal process having the same consequence as a court-issued request for data, in that if we were to refuse to provide such data, it would be in breach of local law, and we or our officers, executives or employees would be subject to liability for failing to honor such legal process;
* Where such disclosure is necessary for us to enforce our legal rights pursuant to applicable law;
* A request for data with the purpose of identifying and/or preventing credit card fraud; or
* Where such disclosure of personal data is necessary to prevent or lessen a serious and imminent threat of bodily or other significant harm to the data subject or other individuals potentially concerned.

**Restoration Services/Third Parties**

We may disclose your information to financial institutions, financial services companies, and other third-parties at your direction to provide restoration services and other Services to you.

If you access third-party services through the Services, these third-party services may be able to collect information about you in accordance with their own privacy policies.

**Corporate Affiliates**

We may share your information with our corporate affiliates.

**Business Transfers**

We may share your information in connection with a substantial corporate transaction, such as the sale of a website, a merger, acquisition, consolidation, asset sale, initial public offering, or in the unlikely event of bankruptcy.

Retention and Deletion of Your Personal Data

We will only retain your personal data for as long as necessary to fulfill the purpose for which the data was collected and is processed, including our compliance with applicable laws, regulations and court orders, and the defense of our legal claims. We will securely dispose of personal data that is no longer needed.

We will hold your personal data on our systems for the longest of the following periods:

* As long as necessary to maintain our ongoing business relationship, or as needed to provide you with the products, services or information which you are entitled to or can otherwise reasonably expect to receive from us;
* For as long as necessary for the purpose for which we collected it or for which you supplied it to us in accordance with any product or service relevant activity or process;
* Any retention period that is necessary to comply with our legal obligations, to resolve disputes, or to enforce our agreements;
* The end of the period in which litigation or investigations might arise in respect of our business relations or other interactions with you;
* At the expiry of the particular personal data retention periods specified by the supplemental information stipulated in certain products’ and services terms and/or notices.

Upon expiry of the applicable retention period, your personal data is either securely disposed of, or de-identified through the use of appropriate anonymization means, including, without limitation, aggregation, truncation, or one-way hashing.

Cross-Border Transfers of Personal Data

When your personal data is transferred internationally within the NortonLifeLock organization or to third-parties, we use legally permitted and sanctioned data transfer mechanisms to ensure that your data remains consistently protected in all places.

We are a global company and, as such, we process data in many countries. To conduct our business, and in accordance with this Statement, your personal data may be transferred to NortonLifeLock and/or its subsidiaries and affiliates in the United States, and to subsidiaries and third-party vendors of NortonLifeLock located worldwide. All transfers will occur in compliance with data transfer requirements of applicable laws and regulations. Where personal data originating from the European Economic Area is transferred to NortonLifeLock subsidiaries and affiliates or to third-party vendors engaged by NortonLifeLock to process such personal data on our behalf who are located in countries that are not recognized by the European Commission as offering an adequate level of personal data protection, such transfers are covered by alternate appropriate safeguards, specifically standard data protection clauses adopted by the European Commission. If applicable to you, you may obtain copies of such safeguards by contacting us as explained below (“Contact Us”).

In the process of continuing to develop our business, we may also occasionally acquire subsidiaries or other business entities. As a result of such transactions, and for maintaining a continued relationship with you, we may transfer your personal data to a related affiliate.

If we are involved in a reorganization, merger, acquisition or sale of our assets, your personal data may be transferred as part of that transaction.

How We Protect Your Personal Data

We implement rigorous physical, technical and organizational safeguards to protect your personal data in our custody, both at rest and in transit, and should these measures fail to prevent a data breach, we will promptly take the necessary remedial measures, and we will notify you as well as applicable regulators of any such breach, as required by applicable law.

Securing personal data is an important aspect of protecting privacy. We take reasonable and appropriate physical, technical, and organizational security measures in accordance with applicable laws to protect your personal data against the risk of accidental loss, compromise, or any form of unauthorized access, disclosure or processing. The relevant security controls are communicated to application owners and technology teams across the business to support the secure development of products and maintain a secure operating environment. Our security measures include:

**Physical Safeguards**

We lock doors and file cabinets, control access to our facilities, implement a clean desk policy, and apply secure destruction to media containing personal data.

**Technical Safeguards**

We endeavor to use reasonably available state-of-the-art network and information security standards, protocols and technologies, including encryption, intrusion detection and data loss prevention, and we monitor our systems and data centers to ensure that they comply with our security policies.

**Organizational Safeguards**

We conduct regular company-wide, as well as role-specific and targeted training and awareness programs on security and privacy, to make sure that our employees and contractors understand the importance of protecting personal data, and that they learn and maintain the necessary knowledge and skills effectively to protect it in practice.

If you have any questions about the security of your personal data or the security of the site, or wish to report a potential security issue, please contact [security@lifelock.com](mailto:security@lifelock.com). When reporting a potential security issue, please describe the matter in as much detail as possible and include any information that might be helpful. If you are having problems accessing your account, please contact our Member Support Center.

Your Privacy Rights

Your Privacy Rights

In relation to our processing of your personal data and subject to applicable law, you may have the rights of information, access (including where applicable portability), rectification, erasure, restriction of and objection to further processing, as well as the rights to withdraw your consent (where consent is the basis of processing) and express other preferences, not to be subjected to automated decision making, and to file privacy complaints with us or with competent authorities.

You can view and update your personal data through your [Norton Account](https://login.norton.com/) or [Lifelock Portal](https://memberportal.lifelock.com/).

Subject to applicable laws, you may have the right:

1) to ask us to provide you with information regarding the personal data we process concerning you;

2) to rectify, update or complement inaccurate or incomplete personal data concerning you;

3) to delete or request the erasure of personal data concerning you;

4) in certain circumstances to restrict the way in which we process personal data concerning you;

5) to withdraw any consent you may have given for us to process personal data concerning you;

6) to object to our processing of personal data concerning you on the basis of our, or of third-parties’ legitimate interests;

7) to obtain from us the portability of personal data concerning you; and

8) to lodge a privacy complaint with a supervisory authority if you are not satisfied with the way we have handled your personal data or any privacy query or request that you have raised with us.

To exercise any of your rights, to raise any other questions, concerns or complaints about our privacy practices or about our use of your personal data and its privacy, or if you are not a customer of ours and want to know what personal data we have about you, please contact us as explained below (“Contact Us”).

Once we receive your request, we will require reasonably sufficient information to verify your identity and your authorization to take the actions requested. You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent to exercise your rights and choices on your behalf, please contact Norton Support in order to verify your identity and verify your authorization for the agent to act on your behalf.

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features available on a Service may change or no longer be available to you where the process of certain data is essential to the provision of the Service or feature. Any difference in the Services are related to the value provided.

Contact Us

You may contact us using multiple communication channels available to you, including by email to nll\_privacy (at) nortonlifelock (dot) com and toll-free to Member Services at 1-800-543-3562.

Americas

* **NortonLifeLock Inc. – Global Privacy Office**  
  60 E. Rio Salado, Suite 1000, Tempe, AZ 85281  
  Email: [nll\_privacy (at) nortonlifelock (dot) com](mailto:nll_privacy@nortonlifelock.com)  
    
  **Member Services:** 1-800-543-3562

Europe – Middle-East – Africa

* **NortonLifeLock Ireland Limited – Global Privacy Office**  
  Ballycoolin Business Park, Blanchardstown, Dublin 15, Ireland  
  Email: [nll\_privacy (at) nortonlifelock (dot) com](mailto:nll_privacy@nortonlifelock.com)
* **Independent EU GDPR Data Protection Officer**  
  Heward Mills, Fitzwilliam Hall  
  Fitzwilliam Place  
  Dublin 2  
  Ireland  
  Email: [DPO (at) nortonlifelock (dot) com](mailto:DPO@nortonlifelock.com)

Referrals, Marketing, Opt-In/Opt-Out, and Cookies

Referrals

In some cases, you may want to refer another person to us, e.g. to try our products or services, or to apply for an open employment position. When doing so, please only share that person’s data with us if you have lawful permission to do so. We will then process that person’s personal data in accordance with this Statement and/or any specific privacy notices and/or job postings.

When you choose to provide us with personal data about third-parties, we will only use this data for the specific reason for which you elect to provide it. It is your responsibility to ensure that when you disclose to us personal data of individuals other than yourself – such as your contacts, your users or other third-parties – you abide by applicable privacy and data security laws, including informing users and third-parties that you are providing their personal data to us, informing them of how it will be transferred, used, or processed, securing appropriate legal permissions and safeguards required for such disclosures, transfers and processing. If you choose to provide us with a third-party's personal data (such as name, email, and phone number), you represent that you have the third-party's permission to do so. Examples include forwarding references or sending job referrals. You also acknowledge that when we interact with such third-party individuals whose personal data you share with us, it is our duty to inform them that we obtained their personal data from you. Where applicable, third-parties may unsubscribe from any future communication following the link provided in the initial message. If you believe that one of your contacts has provided us with your personal data and you would like to request that it be removed from our database, please contact us at nll\_privacy (at) nortonlifelock (dot) com.

Marketing and Community Networking

As permitted by applicable law and subject to your expressed preferences, we process your personal data to communicate with you in order to promote products and services, including via direct messages, interested-based advertisements, through select third-parties, as well as the online NortonLifeLock Community. We may process personal data to determine the effectiveness of our marketing programs and to better tailor them to you. Our marketing communications may include special offers from third-party partners, or joint or bundled offers with third-party partners. The Statement includes information about how to manage your preferences in regard to Marketing Communications.

You may receive marketing messages and materials from us or our affiliates, where and as permitted by applicable law.

You have choices on what communications you wish to receive from us. If you do not want to continue receiving any marketing materials from us, you can click on the unsubscribe function in the communications you receive from us. [You may also unsubscribe from Norton Marketing Offers](https://support.norton.com/sp/en/us/home/current/solutions/v118283428_EndUserProfile_en_us), manage your communication preferences in your [Norton Account](https://login.norton.com/) or [Lifelock Portal](https://memberportal.lifelock.com/), or contact our Member Services Department at 1-800-543-3562 or by regular mail at Attn.: Member Services, 60 East Rio Salado Parkway, Suite 1000, Tempe, AZ 85281. If you choose not to receive marketing communications from us, we will honor your request.

However, we will continue to communicate with you as needed to provide the products and services you are entitled to, to respond to your inquiries, or otherwise relay transactional product or service-related messages.

Please also be aware that you may still receive information about our products and services through other parties using their own mailing lists. For instance, marketing materials for our products and services may also be contained in messages you receive from third-parties which may include your employer if they offer our services as part of their employee benefits, or other service providers that offer our products and services as part of their special offers.

**Interest-Based Ads**

We may provide your data including the data about your interests in our products to third-parties for the purposes of serving you more relevant ads, in accordance with applicable law. Where we provide you with interest-based ads on a site other than our own, we do not track your other activities on that site. If you click on our ads, we will know the domain you came from. For more information, please see the Cookies & Tracking Technologies section below.

**Data from Third-Parties**

Third-parties may provide us with personal data they have collected about you from you or from further online and offline sources, such as marketing data from our partners and third-parties that is combined with information we already have about you, to provide you with more relevant communications and better tailored offers. We make reasonable efforts to verify that the third-parties we engage for such purposes are reputable and law-abiding and we will not solicit them to disclose to us personal data that we do not have a lawful purpose and valid legal basis (e.g., consent, where applicable) to collect and process. However, we are not liable for any processing of your personal data by such third-parties prior to, during or after them providing it to us.

**NortonLifeLock Community (Norton Website Forums, Blogs and Networking Sites)**

We operate forums, websites and related information services, better to assist you in using our Services, discussing technical issues and sharing your experiences. You should be aware that any data you provide in these public forums will not be kept confidential, as it may be read, collected and used by others who access them. To request removal of your personal data from any forum, contact us [here](https://support.norton.com/sp/en/us/home/current/contact-chat?inid=hho_symcom_supp_header). In certain circumstances, we may not be able to remove your personal data, in which case we will let you know why. Please note that your use of these community services may be subject to additional terms and conditions.

How to Opt out of Interest-Based Advertising

You may use a number of third-party tools to opt out of the interest-based tailoring of the ads you see on our websites or of our ads that you see on third-party sites. The full section in this Statement under this topic includes a list of certain opt-out options available to you.

We partner with third-parties to display advertising on our website or to manage our advertising on other sites. You may opt out of many third-party ad networks, including those operated by members of the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA). For more information and available choices for third-party ad networks participating in the NAI and DAA programs, please visit their respective websites: [www.networkadvertising.org/optout\_nonppii.asp](http://www.networkadvertising.org/optout_nonppii.asp) (NAI) and [www.aboutads.info/choices](http://www.aboutads.info/choices) (DAA). If you are in the European Union, you may also do that by visiting Your Online Choices (click [here](http://www.youronlinechoices.eu/)). Please note that if you opt out, you will continue to receive generic ads not based on your interests. Opting out of these networks does not otherwise limit the collection of information described elsewhere in this Policy.

You may control our use of the information we collect about your activities on our websites to display targeted NortonLifeLock advertising during your visits to third-party websites. To opt out of receiving these targeted ads, click [here](https://www.lifelock.com/advertising-choices/). Opting out of participation in our targeted advertising does not opt you out of our use of general information for other purposes, such as analytics supporting optimization of our Site or development of new Services.

Note: If your browser is configured to reject cookies when you visit the opt-out page, or you subsequently erase your cookies, use a different computer or change web browsers, your opt-out may no longer be effective.

Cookies & Tracking Technologies

We use cookies and similar tracking technologies on our websites, as permitted by applicable laws and subject to your consent and choices where relevant. We permit third-parties to activate cookies, features, widgets and other similar technologies on our sites in accordance with applicable law.

**Cookies**

A cookie is a commonly used automated data collection tool. Cookies are small text files that are placed on your computer or device by websites that you visit or HTML-formatted emails you open, to make websites work, or work more efficiently. We and our partners use cookies and other similar tracking technologies (e.g. Web Beacons, JavaScript, clear GIFs, pixel tags, as well as HTML5 and Flash Local Storage Objects) on our websites or emails to:

* Ensure the proper functioning of our websites and the proper delivery of legitimate electronic communications;
* Tailor information presented to you based on your browsing preferences, such as language and geographical region;
* Collect statistics regarding your website usage;
* Provide us with business and marketing information; and
* In some cases, to enable a third-party to deliver future advertising for our products and services to you when you visit certain websites owned by third-parties.

We use different kinds of cookies:

* **Essential cookies** are necessary to provide you with services and features available through our websites. Without these cookies, services you may need, such as shopping carts or e-billing, cannot be provided.
* **Analytics cookies** collect data that is either used in aggregate form to help us understand how the website is being used or the effectiveness of our marketing campaigns.
* **Customization cookies** collect data that is used to help us customize the website for you.
* **Advertising cookies and tracking scripts** are used to make advertising messages more relevant to you. They perform functions like preventing the same ad from continuously reappearing, ensuring that ads are properly delivered and, in some cases, featuring ads based on your interests. On websites which include a cookie management tool, you may find a hover button at the bottom of your screen.

The cookies we use may be session cookies that are erased when you leave our websites, or they may be persistent cookies that remain on your computer's hard drive after you leave the site, in preparation for your next visit.

If you do not wish to receive cookies you may be able to refuse them by not agreeing to the use of them upon entering the website. If you do so, we may be unable to offer you some of our functionalities, services or support. If you have previously visited our websites, you may also have to delete any existing cookies from your browser.

**Third-Party Data Collection**

Cookies may also be placed on our websites by third-parties to deliver tailored information and content which may be of interest to you, such as promotions or offerings, when you visit third-party websites after you have left ours. We do not permit these third-parties to collect personal data about you on our sites beyond such cookies (e.g., email address) unless such data is provided to the third party in their role as a service provider acting solely on our behalf.

**Social Media Features and Widgets**

Our websites include social media features, such as Facebook’s “Like” button, and widgets, such as the “Share This” button, or interactive mini-programs that run on our sites. These features are usually recognizable by their third-party brand or logo and may collect your IP address, which page you are visiting on our websites, and set a cookie to enable the feature to work properly. Any collection of information through such third-party feature is governed by the privacy policy of the company providing it.

**Do-Not-Track Signals and Similar Mechanisms.**

Some mobile and web browsers transmit "do-not-track" signals. Because of differences in how web browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. We currently do not take action in response to these signals.

Automated Individual Decision-Making and Profiling

Unless otherwise specified, NortonLifeLock will only use automated decision making in the interest of network and information security, for the sole purpose of protecting you, NortonLifeLock, our partners and our other customers from cyber-threats, and not for the purpose of evaluating any individual’s personal characteristics.

Where NortonLifeLock processes network traffic data for the purpose of network and information security based on our or our customers’ legitimate interest as outlined in the corresponding section of this Statement, automated decisions concerning particular data elements may occasionally be made. This could involve in particular assigning relative cybersecurity reputation scores to IP addresses and URLs based on objective cyber-threat indicators measured by our and our partners’ cyber-threat detection engines. Such indicators may be for instance the determination that malicious or otherwise harmful contents are hosted at a given URL or are emanating from a given IP address. Such automatically-assigned reputation scores may be leveraged by you, by NortonLifeLock, by our partners and by other customers to detect, block and mitigate the identified cyber-threats. They could therefore result in our products and services blocking network traffic coming from or going to such URLs and IP addresses. No such processing is intended to produce any other effect than protecting you, NortonLifeLock, our partners and our other customers from cyber-threats. Should you nevertheless consider that such automated processing is unduly affecting you in a significant way, please contact us as explained below (“Contact Us”) to raise your concerns and to seek our help in finding a satisfactory solution.

Children’s Privacy

Children’s Privacy

Unless otherwise specified, our websites, products and/or services are not directed at minors (as defined by and in accordance with applicable law). You may add the protection of certain of our Services to minors in your household, but we only process that personal data at your direction and in order to provide those specified Services.

Our websites are not directed to, nor do we knowingly collect data from, minors (as defined by applicable law) except where explicitly described otherwise in the privacy notices of products and services designed specifically for purposes such as to assist you by providing child online protection features. In such cases, we will only collect and process personal data related to any child under 13 years of age which you choose to disclose to us or otherwise instruct us to collect and process. Please refer to the specific applicable notices for important additional information.

Miscellaneous

Changes to this Statement

This Statement does not constitute a contract, and is subject to change, and any material changes that may affect the way we process personal data will be communicated to you. In the case of a material change to our personal data processing practices, any such change will only apply on a going-forward basis; we will not process the personal data currently in our possession in a materially different way without your prior consent.

We reserve the right to revise or modify this Statement. In addition, we may update this Privacy Statement to reflect changes to our data practices. If we make any material changes in the way we collect, process and/or share your personal data, we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. In the case of a material change to our personal data processing practices, any such change will only apply on a going-forward basis; we will not process the personal data currently in our possession in a materially different way without your prior consent. We encourage you to periodically review this page for the latest information on our privacy practices.

Links to Other Websites

If you navigate to third-party websites linked from our websites, please note that those third-parties’ privacy terms (and not NortonLifeLock’s) will apply to your subsequent browsing activity.

Our websites may contain links to other websites, owned or operated by other companies. If you visit any linked websites, please review their privacy statements carefully. We are not responsible for the content or privacy practices of websites that are owned by those third-parties. Our websites may also link to co-branded websites that are maintained by NortonLifeLock and one or more of our business partners, who are collecting your personal data pursuant to their own privacy practices. Please review the applicable privacy statements on any co-branded site you visit, as they may differ from ours.

EFFECTIVE DATE: January 1, 2020

Spotify

**Spotify Datenschutzrichtlinie**

Gültig ab dem 20. Januar 2020

1 [Einführung](https://www.spotify.com/ch-de/legal/privacy-policy/#s1)  
2 [Über diese Datenschutzrichtlinie](https://www.spotify.com/ch-de/legal/privacy-policy/#s2)  
3 [Ihre Rechte und Einstellungen: Wir lassen Ihnen die Wahl und Kontrolle](https://www.spotify.com/ch-de/legal/privacy-policy/#s3)  
4 [Personenbezogene Daten, die wir von Ihnen erheben](https://www.spotify.com/ch-de/legal/privacy-policy/#s4)  
5 [Wofür wir Ihre personenbezogenen Daten verwenden](https://www.spotify.com/ch-de/legal/privacy-policy/#s5)  
6 [Weitergabe Ihrer personenbezogenen Daten](https://www.spotify.com/ch-de/legal/privacy-policy/#s6)  
7 [Datenspeicherung und -löschung](https://www.spotify.com/ch-de/legal/privacy-policy/#s7)  
8 [Übermittlung in andere Länder](https://www.spotify.com/ch-de/legal/privacy-policy/#s8)  
9 [Links](https://www.spotify.com/ch-de/legal/privacy-policy/#s9)  
10 [Schutz Ihrer personenbezogenen Daten](https://www.spotify.com/ch-de/legal/privacy-policy/#s10)  
11 [Kinder](https://www.spotify.com/ch-de/legal/privacy-policy/#s11)  
12 [Änderungen dieser Datenschutzrichtlinie](https://www.spotify.com/ch-de/legal/privacy-policy/#s12)  
13 [Wie Sie uns kontaktieren können](https://www.spotify.com/ch-de/legal/privacy-policy/#s13)

**1. Einführung**

Danke, dass Sie sich für Spotify entschieden haben!

Spotify möchte Ihnen die bestmögliche Erfahrung bieten, um sicherzustellen, dass Sie unseren Service genießen. Dafür müssen wir Ihre Streaming-Gewohnheiten verstehen, damit wir einen außergewöhnlichen und personalisierten Service speziell für Sie anbieten können. Ihre Privatsphäre und die Sicherheit Ihrer personenbezogenen Daten sind äußerst wichtig für uns und werden es auch immer sein. Deshalb möchten wir Ihnen transparent erläutern, wie und warum wir Ihre personenbezogenen Daten sammeln, speichern, weitergeben und nutzen. Außerdem wollen wir Ihnen Ihre Kontroll- und Auswahlmöglichkeiten bezüglich der Frage, wann und wie Sie Ihre personenbezogenen Daten teilen möchten, darlegen.

Das ist unser Ziel, und diese Datenschutzrichtlinie ("Richtlinie") wird im Folgenden genauer erklären, was wir im Detail damit meinen.

**2. Über diese Datenschutzrichtlinie**

Diese Richtlinie erläutert die wesentlichen Details Ihrer Beziehung zu Spotify AB bezüglich Ihrer personenbezogenen Daten. Die Richtlinie gilt für alle Spotify-Dienste und alle zugehörigen Dienste (hier bezeichnet als „Spotify Service"). Die Bedingungen für Ihre Nutzung des Spotify Service sind in unseren [Allgemeinen Nutzungsbedingungen](https://www.spotify.com/ch-de/legal/end-user-agreement/?language=de&country=ch) definiert (die „Nutzungsbedingungen“).

Von Zeit zu Zeit entwickeln wir möglicherweise neue oder zusätzliche Dienstleistungen. Wenn die Einführung dieser neuen oder zusätzlichen Dienstleistungen zu einer wesentlichen Änderung der Art und Weise führt, wie wir Ihre personenbezogenen Daten erheben oder verarbeiten, werden wir Ihnen weitere Informationen oder zusätzliche Bedingungen oder Richtlinien zur Verfügung stellen. Sofern bei der Einführung dieser neuen oder zusätzlichen Dienstleistungen nicht anders angegeben, unterliegen sie dieser Richtlinie.

Ziel dieser Richtlinie ist:

1. sicherzustellen, dass Sie verstehen, welche personenbezogenen Daten wir über Sie erheben, die Gründe, warum wir sie erheben und verwenden und an wen wir sie weitergeben;
2. zu erklären, wie wir die personenbezogenen Daten, die Sie uns zur Verfügung stellen, verwenden, um Ihnen ein großartiges Erlebnis zu bieten, wenn Sie den Spotify Service nutzen; und
3. zu erklären, welche Rechte und Auswahlmöglichkeiten Sie in Bezug auf die personenbezogenen Daten haben, die wir über Sie erheben und verarbeiten, und wie wir Ihre Privatsphäre schützen werden.

Wir hoffen, dass dies Ihnen hilft, unsere Verpflichtungen Ihnen gegenüber im Hinblick auf Ihre Privatsphäre zu verstehen. Für weitere Erläuterungen zu den in dieser Richtlinie verwendeten Begriffen besuchen Sie bitte unser [Datenschutz-Center](https://www.spotify.com/privacy/plain) auf spotify.com. Für Informationen darüber, wie Sie uns kontaktieren können, wenn Sie irgendwann einmal Fragen oder Bedenken haben, schauen Sie bitte im unten stehenden [Abschnitt 13 ‚Wie Sie uns kontaktieren können‘](https://www.spotify.com/ch-de/legal/privacy-policy/#s13). Alternativ, wenn Sie mit dem Inhalt dieser Richtlinie nicht einverstanden sind, denken Sie bitte daran, dass es Ihre Entscheidung ist, ob Sie den Spotify Service nutzen möchten.

**3. Ihre Rechte und Einstellungen: Wir lassen Ihnen die Wahl und Kontrolle**

Die Datenschutzgrundverordnung („DSGVO“) verleiht dem Einzelnen bestimmte Rechte in Bezug auf seine personenbezogenen Daten. Dementsprechend bieten wir Transparenz und Kontrollmöglichkeiten, um den Nutzern die Wahrnehmung dieser Rechte zu erleichtern. Soweit verfügbar und soweit nicht durch das geltende Recht eingeschränkt, sind dem Einzelnen folgende Rechte eingeräumt:

* Auskunftsrecht - das Recht, über die personenbezogenen Daten, die wir über Sie verarbeiten, informiert zu werden und Auskunft dazu zu verlangen;
* Recht auf Berichtigung - das Recht, von uns die Berichtigung oder Aktualisierung Ihrer personenbezogenen Daten zu verlangen, wenn diese ungenau oder unvollständig sind;
* Recht auf Löschung - das Recht, von uns die Löschung Ihrer personenbezogenen Daten zu verlangen;
* Recht auf Einschränkung der Verarbeitung - das Recht, von uns zu verlangen, dass wir die Verarbeitung aller oder einiger Ihrer personenbezogenen Daten vorübergehend oder dauerhaft einstellen;
* Widerspruchsrecht -
  + das Recht, jederzeit der Verarbeitung Ihrer personenbezogenen Daten aus Gründen, die sich aus Ihrer besonderen Situation ergeben, zu widersprechen;
  + das Recht, der Verarbeitung Ihrer personenbezogenen Daten zu Zwecken des Direktmarketings zu widersprechen;
* Recht auf Datenübertragbarkeit - das Recht, eine Kopie Ihrer personenbezogenen Daten in elektronischer Form anzufordern und das Recht, diese personenbezogenen Daten zur Verwendung in dem Dienst einer anderen Partei zu übermitteln; und
* Recht, nicht einer automatisierten Entscheidungsfindung unterworfen zu werden - das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Entscheidungsfindung, einschließlich des Profiling, beruht, wenn die Entscheidung Ihnen gegenüber eine rechtliche Wirkung entfaltet oder Sie in ähnlicher Weise erheblich beeinträchtigt.

Um es Ihnen zu ermöglichen, mehr über diese Rechte zu erfahren, diese Rechte problemlos auszuüben und Ihre Einstellungen in Bezug auf die Art und Weise, wie Spotify Ihre personenbezogenen Daten verwendet, zu speichern, stellen wir die folgenden Mittel zur Verfügung:

* Datenschutz-Einstellungen (zugänglich über Ihre Kontoseite) - ermöglichen es Ihnen, Entscheidungen über die Verarbeitung bestimmter personenbezogener Daten zu treffen und über eine automatische ‚Downloaden Sie Ihre Daten‘-Funktion grundlegende Konto- und Nutzungsinformationen herunterzuladen.
* [Datenschutz-Center](https://www.spotify.com/privacy/plain) - bietet eine bequeme zentrale Stelle, an der Sie weitere Informationen darüber finden können, wie Spotify Ihre personenbezogenen Daten verwendet, Ihre Rechte in Bezug auf Ihre personenbezogenen Daten und wie Sie diese Rechte ausüben können.
* Benachrichtigungs-Einstellungen (zugänglich über Ihre Kontoseite) - ermöglichen es Ihnen auszuwählen, welche Marketingmitteilungen Sie von Spotify erhalten. Sie können diese Einstellungen ändern, um sich für oder gegen den Empfang verschiedener Arten von E-Mail- und Push-Benachrichtigungen zu entscheiden. Bitte beachten Sie, dass E-Mail-Marketing-Nachrichten von Spotify einen Opt-Out-Mechanismus in der Nachricht selbst enthalten (z.B. ein Abmelde-Link in den E-Mails, die wir Ihnen senden). Durch Klicken auf den Link in einer E-Mail werden Sie von weiteren Nachrichten dieser Kategorie ausgenommen (z.B. Artist Updates). Über die Benachrichtigungs-Einstellungen können Sie Entscheidungen über alle Kategorien der E-Mail- und Push-Marketingkommunikation treffen.
* [Cookie-Richtlinie](https://www.spotify.com/ch-de/legal/cookies-policy/?language=de&country=ch) - enthält weitere Informationen darüber, wie wir Cookies verwenden, einschließlich der Verwendung für interessenbezogene Werbung. Sie finden auch Informationen darüber, wie Sie Ihre Cookie-Einstellungen verwalten und bestimmte Arten von Tracking deaktivieren können; und
* Kunden-Support - Wir haben mehrere Seiten auf unserer Kundensupportseite, die weitere Hinweise zu Fragen des Datenschutzes geben. Eine wichtige Informationsquelle ist der Artikel über Datenrechte und Datenschutzeinstellungen, der auch Antworten auf "häufig gestellte Fragen" zur Verarbeitung personenbezogener Daten im Spotify Service enthält.

Wenn Sie Fragen zum Datenschutz, zu Ihren Rechten oder zur Ausübung dieser Rechte haben, wenden Sie sich bitte an unseren Datenschutzbeauftragten über das Formular ‚Kontakt‘ im [Datenschutz-Center](https://www.spotify.com/privacy/plain). Wenn Sie Bedenken bezüglich der Verarbeitung Ihrer personenbezogenen Daten haben, hoffen wir, dass Sie weiterhin mit uns kooperieren, um diese zu lösen. Sie können sich jedoch auch an die schwedische Datenschutzbehörde (Datainspektionen) oder an Ihre örtliche Datenschutzbehörde wenden und haben das Recht, eine Beschwerde einzureichen.

**4. Personenbezogene Daten, die wir von Ihnen erheben**

In den folgenden Tabellen haben wir die Kategorien von personenbezogenen Daten, die wir über Sie erheben und verwenden, und die Art und Weise, wie wir sie erheben, dargestellt:

\* Die folgende Tabelle beschreibt die personenbezogenen Daten, die erhoben werden, wenn Sie sich für den Spotify Service anmelden:\*

| Kategorien personenbezogener Daten | Beschreibung der Kategorie |
| --- | --- |
| Benutzerdaten | Dies sind die personenbezogenen Daten, die von Ihnen zur Verfügung gestellt oder von uns erhoben werden, damit Sie sich für den Spotify Service anmelden und diesen nutzen können. Je nach Art des Spotify Service-Abonnements, für das Sie sich anmelden, kann dies Ihren Benutzernamen, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Geschlecht, Adresse und Land umfassen.  Einige der personenbezogenen Daten, um die wir Sie bitten werden, sind für die Erstellung Ihres Kontos erforderlich. Sie haben auch die Möglichkeit, uns zusätzliche personenbezogenen Daten zur Verfügung zu stellen, um Ihr Konto stärker zu personalisieren.  Die Art und der Umfang der von uns erhobenen personenbezogenen Daten hängen davon ab, für welche Art von Spotify Service-Abonnement Sie sich anmelden, wie Sie ein Konto erstellen und ob Sie Dienste Dritter (wie z.B. Facebook) nutzen, um sich anzumelden und den Spotify Service zu nutzen. Wenn Sie einen Drittanbieterdienst zur Erstellung eines Kontos verwenden, erhalten wir personenbezogene Daten über diesen Drittanbieterdienst, aber nur, wenn Sie der Weitergabe Ihrer personenbezogenen Daten an uns durch diesen Drittanbieterdienst zugestimmt haben. Bitte beachten Sie, dass die verfügbaren Abonnements und Anmeldeoptionen von Land zu Land unterschiedlich sein können. |

*Die folgende Tabelle beschreibt personenbezogene Daten, die durch Ihre Nutzung des Spotify Service erhoben werden:*

| Kategorien personenbezogener Daten | Beschreibung der Kategorie |
| --- | --- |
| Nutzungsdaten | Dies sind die personenbezogenen Daten, die über Sie erhoben werden, wenn Sie den Spotify Service aufrufen und/oder nutzen, einschließlich:   * Informationen über die Art Ihres Spotify Service-Abonnements. * Informationen über Ihre Interaktionen mit dem Spotify Service, wie z.B. Ihre Suchanfragen (einschließlich Datum und Uhrzeit Ihrer Anfragen), Streaming-Verlauf, von Ihnen erstellte Playlisten, Ihre Bibliothek, Ihr Browserverlauf und Ihre Interaktionen mit dem Spotify Service, Inhalten, anderen Spotify-Nutzern. Dies kann auch Details über Ihre Nutzung von Anwendungen Dritter in Verbindung mit dem Spotify Service enthalten. * Rückschlüsse auf Ihre Interessen und Präferenzen basierend auf Ihrer Nutzung des Spotify Service. * Nutzergenerierte Inhalte (im Sinne der [Nutzungsbedingungen](https://www.spotify.com/ch-de/legal/end-user-agreement/?language=de&country=ch)), die Sie auf Spotify posten, wie z.B. Fotos, Playlist-Titel und Interaktionen mit der Spotify Kundenbetreuung. Bitte beachten Sie, dass wir nur dann auf die Kamera oder die Fotos auf Ihrem Gerät zugreifen werden, wenn Sie uns die Erlaubnis dazu erteilen. Wir werden nur auf Bilder zugreifen, die Sie ausdrücklich für die Weitergabe an uns ausgewählt haben, sowie auf Metadaten, die sich auf diese Bilder beziehen, wie z. B. den Dateityp und die Größe des Bildes. Wir werden niemals die Fotobibliothek oder die Kamera Ihres Geräts scannen oder importieren. * Bestimmte technische Daten, wie z.B.:   + URL-Informationen;   + Online-Identifikatoren einschließlich Cookie-Daten und IP-Adressen;   + Informationen über die von Ihnen verwendeten Gerätetypen, wie z. B. eindeutige Geräte-IDs, Netzwerkverbindungstyp (z. B. Wifi, 3G, LTE, Bluetooth), Provider, Netzwerk- und Geräteleistung, Browsertyp, Sprache, Informationen zur Ermöglichung der Verwaltung digitaler Rechte, Betriebssystem und Version der Spotify-Anwendung;   + Geräteattribute von Geräten in Ihrem Wifi-Netzwerk, die für die Verbindung mit dem Spotify Service verfügbar sind (wie z.B. Lautsprecher);   + ihr nicht exakter Standort, der aus bestimmten technischen Daten (z.B. Ihrer IP-Adresse, der Spracheinstellung Ihres Geräts oder der Zahlungswährung) abgeleitet oder geschlussfolgert werden kann, um geografische Anforderungen in unseren Lizenzvereinbarungen zu erfüllen und Ihnen personalisierte Inhalte und Werbung zu liefern; und   + bewegungsgenerierte oder orientierungsgenerierte mobile Sensordaten (z.B. Beschleunigungssensor oder Gyroskop), die für die Bereitstellung bestimmter Funktionen des Spotify Service erforderlich sind. |
| Daten zur Verifizierung des Abonnements | Für Nutzer bestimmter Abonnements wie dem Premium Family-Abonnement und dem Premium DuoAbonnement nutzen wir möglicherweise eine Kartenanwendung eines Drittanbieters (z. B. Google Maps) und/oder den Standortservice Ihres Geräts, um Ihnen bei der Verifizierung Ihrer Adresse zu helfen. Diese Daten werden ausschließlich zum Zweck der Verifizierung der Nutzungsberechtigung für das Premium Family-Abonnement und das Premium Duo-Abonnement erhoben und nicht für Werbe- oder andere Zwecke verwendet. |

\*Die folgende Tabelle beschreibt personenbezogene Daten, bei denen Sie sich dazu entschieden haben, uns diese zur Verfügung zu stellen, damit wir Ihnen zusätzliche Features/Funktionalitäten anbieten können \*

| Kategorien personenbezogener Daten | Beschreibung der Kategorie |
| --- | --- |
| Sprachdaten | Wenn Sprachfunktionen in Ihrem Markt verfügbar sind, sammeln wir mit Ihrer Erlaubnis Ihre Sprachdaten, um Ihnen zusätzliche Features und Funktionalitäten zur Verfügung zu stellen, wie z.B. die Interaktion mit dem Spotify Service mittels Ihrer Stimme. Weitere Informationen finden Sie in unserer [Sprachsteuerungsrichtlinie](https://www.spotify.com/ch-de/legal/voice-controls/?language=de&country=ch). |
| Zahlungs- und Kaufdaten | Wir erheben möglicherweise bestimmte personenbezogene Daten, wenn Sie sich für ein Probeabonnement anmelden, eines unserer kostenpflichtigen Abonnements (im Sinne der [Nutzungsbedingungen](https://www.spotify.com/ch-de/legal/end-user-agreement/?language=de&country=ch)) erwerben oder andere Käufe über den Spotify Service tätigen. Die dabei erhobenen genauen personenbezogenen Daten werden je nach Zahlungsart (z.B. direkt über Ihren Mobilfunkanbieter oder per Rechnung) unterschiedlich sein, beinhalten aber Informationen wie z.B.:   * Name; * Geburtsdatum; * Kredit- oder Debitkartentyp, Ablaufdatum und bestimmte Ziffern Ihrer Kartennummer; * Postleitzahl; * Handynummer; und * Details zu Ihrer Kauf- und Zahlungshistorie. |
| Daten zu Wettbewerben, Umfragen und Gewinnspielen | Wenn Sie Formulare ausfüllen, auf eine Umfrage oder einen Fragebogen antworten oder an einem Wettbewerb teilnehmen, erheben wir die von Ihnen angegebenen personenbezogenen Daten. |

\*Die folgende Tabelle beschreibt personenbezogene Daten, die wir über Drittquellen sammeln \*

Wir erheben personenbezogene Daten über Sie von verschiedenen Dritten. Diese Drittquellen variieren im Laufe der Zeit und umfassen die folgenden:

| Kategorien von Drittquellen | Beschreibung der Kategorie |
| --- | --- |
| Authentifizierungspartner | Wenn Sie sich mit den Zugangsdaten Dritter (z.B. Facebook) bei unseren Diensten registrieren oder einloggen, werden wir Ihre Informationen von diesen Dritten importieren, um Ihr Konto bei uns zu erstellen. |
| Technische Servicepartner | Wir arbeiten mit technischen Servicepartnern zusammen, die uns bestimmte Daten zur Verfügung stellen, wie z.B. die Zuordnung von IP-Adressen zu nicht exakten Standortdaten (z.B. Stadt, Bundesland), damit wir den Spotify Service, Inhalte und Funktionen bereitstellen können. |
| Zahlungspartner | Wenn Sie sich dafür entscheiden, für eine Dienstleistung oder ein Feature per Rechnung zu bezahlen, erhalten wir möglicherweise Daten von unseren Zahlungspartnern, damit wir Ihnen Rechnungen schicken, Ihre Zahlung bearbeiten und Ihnen zur Verfügung stellen können, was Sie gekauft haben. |
| Werbetreibende und andere Werbepartner | Möglicherweise erhalten wir bestimmte Daten über Sie, wie z.B. Cookie-ID, Mobilgeräte-ID oder E-Mail-Adresse, sowie Rückschlüsse auf Ihre Interessen und Präferenzen von bestimmten Werbetreibenden und Werbepartnern, die es uns ermöglichen, relevantere Werbung zu liefern und deren Wirksamkeit zu messen. |

**5. Wofür wir Ihre personenbezogenen Daten verwenden**

Wenn Sie den Spotify Service nutzen oder mit ihm interagieren, verwenden wir eine Vielzahl von Technologien, um die personenbezogenen Daten zu verarbeiten, die wir aus verschiedenen Gründen über Sie erheben. In der folgenden Tabelle haben wir die Gründe für die Verarbeitung Ihrer personenbezogenen Daten, die zugrundeliegenden Rechtsgrundlagen, auf die wir uns stützen, um Ihre personenbezogenen Daten verarbeiten zu können, sowie die Kategorien der personenbezogenen Daten (ausgewiesen in [Abschnitt 4 ‚Personenbezogene Daten, die wir von Ihnen erheben‘](https://www.spotify.com/ch-de/legal/privacy-policy/#S4), die für diese Zwecke verwendet werden, aufgeführt:

| Beschreibung, wozu Spotify Ihre personenbezogenen Daten verarbeitet (‚Verarbeitungszweck‘) | Rechtsgrundlage für den Verarbeitungszweck | Kategorien von personenbezogenen Daten, die Spotify für den Verarbeitungszweck verwendet |
| --- | --- | --- |
| Zur Bereitstellung und Personalisierung des Spotify Service. | * Erfüllung eines Vertrages * Berechtigtes Interesse * Einwilligung | * Benutzerdaten * Nutzungsdaten * Zahlungs- und Kaufdaten * Daten zur Verifizierung des Abonnements * Sprachdaten |
| Um Probleme mit dem Spotify Service zu verstehen, zu diagnostizieren, zu behandeln und zu beheben. | * Erfüllung eines Vertrages * Berechtigtes Interesse | * Benutzerdaten * Nutzungsdaten |
| Für die Bewertung und Entwicklung neuer Funktionen, Technologien und Verbesserung des Spotify Service. | * Berechtigtes Interesse * Einwilligung | * Benutzerdaten * Nutzungsdaten * Sprachdaten |
| Für Marketing-, Promotions- und Werbezwecke. | * Berechtigtes Interesse * Einwilligung | * Benutzerdaten * Nutzungsdaten * Sprachdaten |
| Um rechtliche Verpflichtungen und Anfragen der Strafverfolgungsbehörden zu erfüllen. | * Erfüllung einer rechtlichen Verpflichtung * Berechtigtes Interesse | * Benutzerdaten * Nutzungsdaten * Zahlungs- und Kaufdaten * Daten zur Verifizierung des Abonnements * Sprachdaten * Wettbewerbs-, Umfrage- und Gewinnspieldaten |
| Zur Erfüllung vertraglicher Verpflichtungen mit Dritten, z.B. Lizenzvereinbarungen, und zur Ergreifung geeigneter Maßnahmen im Hinblick auf Berichte über die Verletzung von geistigem Eigentum und unangemessenen Inhalten. | * Berechtigtes Interesse | * Benutzerdaten * Nutzungsdaten * Zahlungs- und Kaufdaten |
| Zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen. | * Berechtigtes Interesse | * Benutzerdaten * Nutzungsdaten * Zahlungs- und Kaufdaten * Daten zur Verifizierung des Abonnements * Sprachdaten * Wettbewerbs-, Umfrage- und Gewinnspieldaten |
| Zur Durchführung von Geschäftsplanung, Berichterstattung und Prognosen. | * Berechtigtes Interesse | * Benutzerdaten * Nutzungsdaten * Zahlungs- und Kaufdaten |
| Zur Abwicklung Ihrer Zahlungen. | * Erfüllung eines Vertrages * Erfüllung einer rechtlichen Verpflichtung | * Benutzerdaten * Zahlungs- und Kaufdaten |
| Um Betrug, einschließlich betrügerischer Zahlungen und betrügerischer Nutzung des Spotify Service, aufzudecken. | * Erfüllung eines Vertrags * Erfüllung einer rechtlichen Verpflichtung * Berechtigtes Interesse | * Benutzerdaten * Nutzungsdaten * Zahlungs- und Kaufdaten * Daten zur Verifizierung des Abonnements |
| Um Forschung, Wettbewerbe, Umfragen und Gewinnspiele durchzuführen. | * Erfüllung eines Vertrages * Berechtigtes Interesse * Einwilligung   F   * Benutzerdaten * Nutzungsdaten * Wettbewerbs-, Umfrage- und Gewinnspieldaten |  |

Wenn Sie weitere Informationen über die Interessenabwägung benötigen, die Spotify zur Rechtfertigung seines Rückgriffs auf die Rechtsgrundlage des berechtigten Interesses gemäß der DSGVO vorgenommen hat, entnehmen Sie bitte [Abschnitt 13 ‚Wie Sie uns kontaktieren können‘](https://www.spotify.com/ch-de/legal/privacy-policy/#S13) weitere Details für die Kontaktaufnahme.

**6. Weitergabe Ihrer personenbezogenen Daten**

Wir haben die Kategorien von Empfängern der personenbezogenen Daten, die durch Ihre Nutzung des Spotify Service erhoben oder generiert werden, aufgeführt.

*Öffentlich zugängliche Informationen*

Die folgenden personenbezogenen Daten werden auf dem Spotify Service stets öffentlich zugänglich sein: Ihr Name und/oder Benutzername, Ihr Profilbild, wem Sie auf dem Spotify Service folgen und wer Ihnen folgt, Ihre zuletzt abgespielten Künstler und Ihre öffentlichen Playlists.

*Personenbezogene Daten, die Sie freiwillig teilen können*

Die folgenden personenbezogenen Daten werden nur an die Kategorien von Empfängern, die unten in der Tabelle aufgeführt sind, weitergegeben, wenn:

* Sie sich dafür entscheiden, eine bestimmte Funktion des Spotify Service zu benutzen, für deren Nutzung die Weitergabe der spezifischen personenbezogenen Daten notwendig ist; oder
* Sie uns Ihre Erlaubnis zur Weitergabe der personenbezogenen Daten erteilen, z.B. indem Sie die entsprechende Einstellung im Spotify Service wählen oder Spotify über einen angezeigten Einwilligungsmechanismus autorisieren.

| Kategorien von Empfängern | Grund für die Weitergabe |
| --- | --- |
| Anwendungen und Geräte von Drittanbietern, die Sie mit Ihrem Spotify-Konto verbinden | Wenn Sie Ihr Spotify-Konto mit einer Anwendung und/oder einem Gerät eines Drittanbieters verbinden, wie z.B. Social Media-, Audio-, Fernseh- oder Fahrzeug-Plattformen und -Dienste, gibt Spotify technische Daten an den Betreiber dieser Drittanbieteranwendung und/oder dieses Drittanbietergeräts weiter, um Ihr Spotify-Konto zu verbinden und/oder die Wiedergabe des Spotify Service zu erleichtern. In Bezug auf bestimmte Dritte, die möglicherweise darum bitten oder verlangen, dass wir Ihre Daten an sie weitergeben, wird Ihre Erlaubnis eingeholt, bevor wir Ihre Daten an diese Dritten weitergeben. |
| Support Community | Wenn Sie ein Spotify Support-Konto in der Spotify Support Community anlegen, fordern wir Sie auf, einen für die Spotify Support Community spezifischen Benutzernamen anzulegen. Dieser wird allen, die auf die Spotify Support Community zugreifen, zusammen mit allen Fragen bzw. Kommentaren, die Sie posten, öffentlich angezeigt. |
| Ihre Spotify Follower | Es kann vorkommen, dass Sie möchten, dass wir Informationen über Ihre Nutzung des Spotify Service mit anderen Spotify-Nutzern, auch „Deine Spotify Follower“ genannt, teilen. Zum Beispiel haben Sie die Möglichkeit, sowohl private als auch öffentliche Playlists zu erstellen. Wenn Sie Ihre privaten Playlists mit anderen teilen, beachten Sie bitte, dass die Empfänger Ihrer privaten Playlists diese Playlists wiederum mit anderen teilen können. |
| Künstler und Plattenlabel | Sie können sich dafür entscheiden, personenbezogene Daten (z.B. Ihre E-Mail-Adresse) an Künstler, Plattenfirmen oder andere Partner weiterzugeben, die Ihnen direkt News oder Werbeangebote zusenden möchten. Sie haben jederzeit die Möglichkeit, Ihre Meinung zu ändern und Ihre Einwilligung zu widerrufen. |

Weitere Informationen über die Handhabung von Benachrichtigungen, Ihre öffentlich verfügbaren Informationen und was Sie mit anderen teilen, finden Sie in [Abschnitt 3 ‚Ihre Rechte und Einstellungen: Wir lassen Ihnen die Wahl und Kontrolle’](https://www.spotify.com/ch-de/legal/privacy-policy/#S3) dieser Richtlinie und im [Datenschutz-Center](https://www.spotify.com/privacy/plain).

*Informationen, die wir weitergeben können*

| Kategorien von Empfängern | Grund für die Weitergabe |
| --- | --- |
| Dienstleister | Wir arbeiten mit Dienstleistern zusammen, die in unserem Auftrag arbeiten und möglicherweise Zugang zu bestimmten personenbezogenen Daten benötigen, um ihre Dienstleistungen für uns erbringen zu können. Zu diesen Unternehmen gehören diejenigen, die wir beauftragt haben, um den Kundenbetreuungs-Support bereitzustellen, die technische Infrastruktur zu betreiben, die wir für die Bereitstellung des Spotify Service benötigen, beim Schutz und der Sicherung unserer Systeme und Dienste zu helfen und die Vermarktung der eigenen Produkte und Dienste von Spotify sowie der Produkte, Dienste, Veranstaltungen von Partnern sowie von Co-branding Aktionen, an denen Spotify beteiligt ist, zu unterstützen. |
| Zahlungsabwickler | Wir werden Ihre personenbezogenen Daten an unsere Zahlungsabwickler weitergeben, soweit dies zur Abwicklung Ihrer Zahlungen und zur Betrugsbekämpfung erforderlich ist. |
| Werbepartner | Wir arbeiten mit Werbepartnern zusammen, damit wir die Werbeinhalte, die Sie gegebenenfalls auf dem Spotify Service erhalten können, individuell anpassen können. Diese Partner helfen uns dabei, Ihnen relevantere Anzeigen und Werbebotschaften anzuzeigen, die interessenbezogene Werbung (auch bekannt als Online Behavioral Advertising), kontextbezogene Werbung und generische Werbung auf dem Spotify Service umfassen können. Wir und unsere Werbepartner können bestimmte personenbezogene Daten verarbeiten, um Spotify dabei zu helfen, Ihre Interessen oder Einstellungen zu verstehen, damit wir Ihnen Werbung liefern können, die für Sie relevanter ist. |
| Spotify-Partner | Je nachdem, wie Sie sich für den Spotify Service anmelden (z.B. über einen Drittanbieter oder einen Mobilfunkanbieter), geben wir Ihren Spotify-Benutzernamen oder andere Benutzerdaten weiter, wenn dies zur Aktivierung Ihres Kontos erforderlich ist. Wir können auch personenbezogene Daten bezüglich Ihrer Nutzung des Spotify Service an diese Drittpartei weitergeben, wie z.B. ob und in welchem Umfang Sie das Angebot genutzt, ein Spotify-Konto aktiviert oder den Spotify Service aktiv genutzt haben. Wir können Ihre personenbezogenen Daten möglicherweise auch an unsere Partner in der Musikindustrie in einem pseudonymisierten Format weitergeben, um diesen zu helfen zu verstehen, wie die Inhalte, die sie an uns lizenzieren, funktionieren und damit Sie die Möglichkeit haben, über den Spotify Service Streaming-Inhalte anzuhören. |
| Wissenschaftliche Forschungen | Wir werden Ihre personenbezogenen Daten für Aktivitäten wie statistische Analysen und akademische Studien weitergeben, jedoch nur in pseudonymisierter Form. |
| Andere Spotify-Konzerngesellschaften | Wir werden Ihre personenbezogenen Daten an andere Unternehmen der Spotify-Gruppe weitergeben, um unsere täglichen Geschäftsvorgänge durchzuführen und um es uns zu ermöglichen, den Spotify Service für Sie aufrechtzuerhalten und bereitzustellen. |
| Strafverfolgungs- und Datenschutzbehörden | Wir geben Ihre personenbezogenen Daten weiter, wenn wir nach Treu und Glauben der Ansicht sind, dass dies für uns notwendig ist, um einer gesetzlichen Verpflichtung nach geltendem Recht nachzukommen oder im Rahmen eines gerichtlichen Verfahrens zu reagieren, wie z.B. einen Durchsuchungsbefehl, einen Gerichtsbeschluss oder eine Vorladung. Wir geben Ihre personenbezogenen Daten auch dann weiter, wenn wir nach Treu und Glauben davon ausgehen, dass dies für unsere eigenen oder die berechtigten Interessen Dritter im Hinblick auf die nationale Sicherheit, die Strafverfolgung, Rechtsstreitigkeiten, strafrechtliche Ermittlungen, den Schutz der Sicherheit einer Person oder zur Verhinderung von Tod oder drohender Körperverletzung erforderlich ist, sofern wir der Auffassung sind, dass Ihre Interessen oder Ihre Grundrechte und -freiheiten, die den Schutz Ihrer personenbezogenen Daten erfordern, nicht überwiegen. |
| Erwerber unseres Unternehmens | Wir werden Ihre personenbezogenen Daten in den Fällen weitergeben, in denen wir unser Unternehmen an einen Käufer oder Kaufinteressenten verkaufen oder über einen Verkauf verhandeln. In dieser Situation wird Spotify weiterhin die Vertraulichkeit Ihrer personenbezogenen Daten sicherstellen und Sie benachrichtigen, bevor Ihre personenbezogenen Daten an den Käufer übertragen werden oder einer anderen Datenschutzrichtlinie unterliegen. |

**7. Speicherung und Löschung von Daten**

Wir bewahren Ihre personenbezogenen Daten nur so lange auf, wie es für die Bereitstellung des Spotify Service und für legitime und wesentliche Geschäftszwecke erforderlich ist, wie z.B. die Aufrechterhaltung der Leistung des Spotify Service, das Treffen datengesteuerter Geschäftsentscheidungen über neue Funktionen und Angebote, die Einhaltung unserer rechtlichen Verpflichtungen und die Beilegung von Streitigkeiten. Wir bewahren einige Ihrer personenbezogenen Daten so lange auf, wie Sie Nutzer des Spotify Service sind. Zum Beispiel bewahren wir Ihre Playlists, Ihre Songbibliothek und Ihre Kontoinformationen auf.

Wenn Sie dies verlangen, löschen oder anonymisieren wir Ihre personenbezogenen Daten, so dass Sie nicht mehr identifizierbar sind, es sei denn, wir sind gesetzlich berechtigt oder verpflichtet, bestimmte personenbezogene Daten vorzuhalten, z. B. in folgenden Situationen:

* Wenn es ein ungelöstes Problem in Bezug auf Ihr Konto gibt, wie z.B. ein ausstehendes Guthaben auf Ihrem Konto oder eine ungeklärte Forderung oder Streitigkeit, werden wir die notwendigen personenbezogenen Daten aufbewahren, bis das Problem gelöst ist;
* Soweit wir die personenbezogenen Daten für unsere rechtlichen, steuerlichen, prüfungstechnischen und buchhalterischen Verpflichtungen benötigen, werden wir die erforderlichen personenbezogenen Daten für den gesetzlich vorgeschriebenen Zeitraum aufbewahren; und/oder,
* Soweit es für unsere berechtigten Geschäftsinteressen wie z.B. zur Vermeidung von Betrug oder zur Wahrung der Sicherheit unserer Nutzer erforderlich ist.

**8. Übermittlung in andere Länder**

Spotify gibt Ihre personenbezogenen Daten weltweit an die Unternehmen der Spotify-Gruppe weiter, um die in dieser Richtlinie aufgeführten Aktivitäten durchzuführen. Spotify kann die Verarbeitung Ihrer personenbezogenen Daten auch durch Unteraufträge an Dritte in anderen Ländern als Ihrem Land vergeben oder ihre personenbezogenen Daten an solche Dritte weitergeben. Ihre personenbezogenen Daten können daher Datenschutzgesetzen unterliegen, die sich von denjenigen in Ihrem Land unterscheiden.

Personenbezogene Daten, die innerhalb der Europäischen Union und der Schweiz erhoben werden, können z.B. an Dritte, die in einem Land außerhalb der Europäischen Union und der Schweiz ansässig sind, übermittelt und von diesen verarbeitet werden. In diesen Fällen stellt Spotify sicher, dass die Übermittlung Ihrer personenbezogenen Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgt und insbesondere, dass angemessene vertragliche, technische und organisatorische Maßnahmen, wie zum Beispiel die von der EU-Kommission genehmigten Standardvertragsklauseln, vorhanden sind.

Weitere Einzelheiten zu den Sicherheitsmaßnahmen, die wir zum Schutz Ihrer personenbezogenen Daten einsetzen, finden Sie in [Abschnitt 10 ‚Schutz Ihrer personenbezogenen Daten‘](https://www.spotify.com/ch-de/legal/privacy-policy/#s10) dieser Richtlinie.

**9. Links**

Wir können Werbung von Dritten und andere Inhalte anzeigen, die auf Webseiten Dritter verweisen. Wir können die Datenschutzpraktiken und Inhalte Dritter weder kontrollieren noch für diese verantwortlich gemacht werden. Wenn Sie auf die Werbung oder den Link eines Dritten klicken, beachten Sie bitte, dass Sie den Spotify Service verlassen und dass alle personenbezogenen Daten, die Sie zur Verfügung stellen, nicht durch diese Richtlinie abgedeckt sind. Bitte lesen Sie die Datenschutzrichtlinien der Dritten, um herauszufinden, wie diese Ihre personenbezogenen Daten erheben und verarbeiten.

**10. Schutz Ihrer personenbezogenen Daten**

Wir sind dem Schutz der personenbezogenen Daten unserer Nutzer verpflichtet. Wir setzen angemessene technische und organisatorische Maßnahmen ein, um die Sicherheit Ihrer personenbezogenen Daten zu gewährleisten; bitte beachten Sie jedoch, dass kein System jemals vollkommen sicher ist. Wir haben verschiedene Richtlinien implementiert, darunter Pseudonymisierungs-, Verschlüsselungs-, Zugangs- und Aufbewahrungsrichtlinien, um unbefugten Zugriff und unnötige Speicherung von personenbezogenen Daten in unseren Systemen zu verhindern.

Ihr Passwort schützt Ihr Benutzerkonto, daher empfehlen wir Ihnen, ein sicheres Passwort zu verwenden, das nur für Ihr Spotify-Konto gilt, Ihr Passwort niemals an Dritte weiterzugeben, den Zugang zu Ihrem Computer und Browser zu beschränken und sich nach der Nutzung des Spotify Service auszuloggen.

**11. Kinder**

Mit Ausnahme von Spotify Kids, einer separaten Spotify-Anwendung, die in bestimmten Märkten verfügbar ist, ist der Spotify Service nicht an Kinder unter 13 Jahren gerichtet. Der Spotify Service wird auch nicht für Kinder angeboten, deren Alter die Verarbeitung ihrer personenbezogenen Daten illegal macht oder nach der DSGVO oder anderen lokalen Gesetzen die Zustimmung der Eltern zur Verarbeitung ihrer personenbezogenen Daten erfordert.

Wir erheben wissentlich keine personenbezogenen Daten von Kindern unter 13 Jahren oder unter der einschlägigen Altersgrenze (die „Altersgrenze“). Wenn Sie unter der Altersgrenze sind, nutzen Sie den Spotify Service bitte nicht und stellen Sie uns keine personenbezogenen Daten zur Verfügung.

Wenn Sie ein Elternteil eines Kindes unter der Altersgrenze sind und feststellen, dass Ihr Kind personenbezogene Daten an Spotify übermittelt hat, kontaktieren Sie uns bitte über das Formular ‚Kontakt‘ im [Datenschutz-Center](https://www.spotify.com/privacy/plain), und Sie können die Ausübung Ihrer geltenden Rechte verlangen, die in [Abschnitt 3 ‚Ihre Rechte und Einstellungen: Wir lassen Ihnen die Wahl und Kontrolle‘](https://www.spotify.com/ch-de/legal/privacy-policy/#s3) dieser Richtlinie beschrieben sind.

Wenn wir erfahren, dass wir die personenbezogenen Daten eines Kindes unter 13 Jahren erhoben haben, werden wir angemessene Maßnahmen ergreifen, um die personenbezogenen Daten zu löschen. Dies kann dazu führen, dass wir das Spotify-Konto für dieses Kind löschen müssen.

**12. Änderungen dieser Datenschutzrichtlinie**

Möglicherweise werden wir gelegentlich Änderungen an dieser Richtlinie vornehmen.

Wenn wir wesentliche Änderungen an dieser Richtlinie vornehmen, werden wir Sie ausdrücklich hierüber informieren in einer Form, die unter den gegebenen Umständen angemessen ist, z.B. indem wir eine hervorgehobene Mitteilung innerhalb des Spotify Service anzeigen oder Ihnen eine E-Mail und/oder eine Gerätebenachrichtigung senden. Möglicherweise werden wir Sie im Voraus benachrichtigen.

Bitte stellen Sie daher sicher, dass Sie solche Mitteilungen sorgfältig lesen.

Wenn Sie mehr über diese Richtlinie und die Verwendung Ihrer personenbezogenen Daten durch Spotify erfahren möchten, besuchen Sie bitte das [Datenschutz-Center](https://www.spotify.com/privacy/plain) auf spotify.com.

**13. Wie Sie uns kontaktieren können**

Danke, dass Sie unsere Richtlinie gelesen haben. Wenn Sie Fragen zu dieser Richtlinie haben, wenden Sie sich bitte an unseren Datenschutzbeauftragten, indem Sie das Formular ‚Kontakt‘ im [Datenschutz-Center](https://www.spotify.com/privacy/plain) verwenden, eine E-Mail an [privacy@spotify.com](mailto:privacy@spotify.com) senden, oder uns an folgende Adresse schreiben:  
  
Spotify AB  
Regeringsgatan 19  
111 53 Stockholm  
Schweden

**KASPERSKY LAB PRIVACY POLICY FOR WEBSITES**

Last updated: 04/28/2020. [What’s New](https://www.kaspersky.com/web-privacy-policy/updates)

**DATA CONTROLLER INFORMATION**

This privacy policy applies to AO Kaspersky Lab, located at bldg. 3, 39A, Leningradskoe Shosse, Moscow, 125212, Russian Federation (“Kaspersky”, “Kaspersky Lab” or “we”) websites that receive data and are linking to this Privacy Policy. It does not apply to Kaspersky websites that do not display or link to this Privacy Policy or that have their own Privacy Policy. It also does not apply to Kaspersky Lab’s services and products unless they are linking to this Privacy Policy.

In this Privacy Policy we inform you about the processing and the privacy of your personal data when using our websites. As a security expert company, data privacy and data security are very important to us. Therefore, we are committed to respecting and protecting your privacy and to handling your personal data confidentially. We recommend visiting this website regularly as this Privacy Policy can be updated due to possible amendments to the law or changes of our internal processes.

If you have any questions or comments regarding the processing of your personal information and Kaspersky's privacy practices or if you would like us to update information or preferences you provided to us, please contact our data protection officer at <https://support.kaspersky.com/general/privacy> or directly by post or email: Kaspersky Labs GmbH, Ingolstadt, Despag-Strasse 3, 85055, Germany, [dpo@kaspersky.com](mailto:dpo@kaspersky.com).

You can also contact Kaspersky EU representative (in accordance with Article 27 GDPR): Kaspersky Labs GmbH, Ingolstadt, Despag-Strasse 3, 85055, Germany, [info@kaspersky.de](mailto:info@kaspersky.de), +49 (0) 841 98 18 90.

**GENERAL INFORMATION**

In general, you can visit and read most parts of our website contents without providing any personal data.

For the process of retrieving your requested information from our websites, our servers store certain data needed for service delivery and/or for statistical or security purposes in anonymized or pseudonymized form (pseudonymized form means data is collected under a pseudonym, i.e. a unique random alphanumeric string generated internally in order to identify each data record). In this context, general information is recorded, such as your domain name or browser type. These data do not enable us to draw conclusions regarding your identity. These anonymized or pseudonymized data are deleted promptly after their statistical evaluation.

We do not process any “Special Categories of Personal Data” about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data).

**Notice for California Consumers.** If you are looking for CCPA-specific information, check out our [CCPA Privacy Notice](https://www.kaspersky.com/web-privacy-policy/ccpa) as well, which is incorporated into this Privacy Policy.

**WHY WE PROCESS YOUR PERSONAL DATA**

The purposes for processing the personal data that you provide depend on the websites, services and features you use. In particular, we use the data to:

* ensure the performance of a contract with users and to ensure the required performance of services for customers;
* protect the user from known threats to information security;
* improve user interaction and experience with our services, in particular, changing interfaces and providing the desired content and advertisements related to marketing purpose;
* provide technical support of products and services for customers and to improve the quality of products and services;
* respond to your questions and otherwise Interact with you;
* secure our websites and protect you and us against fraud.

**WHAT IS OUR LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA**

Our lawful basis for processing your general personal data:

* processing necessary for the performance of a contract with the data subject or to take steps to enter into a contract;
* where it is necessary for our legitimate interests and your interests and fundamental rights do not conflict with those interests:
  + in ensuring the ongoing security and proper operation of our website and associated IT systems and prevent fraud;
  + limited personal data is stored in case the individuals have asked us to not process their personal data to ensure that the Kaspersky Lab can remain compliant with their request.
* your specific consent to process for the Purpose in question;
* processing necessary for compliance with a legal obligation.

**AUTOMATED DECISION MAKING**

We do not use automated decision making at our Websites and Services.

**WHAT PERSONAL DATA DO WE PROCESS AND HOW DO WE USE IT**

**[My Kaspersky](https://my.kaspersky.com/),**[**Kaspersky Account**](https://account.uis.kaspersky.com/)**,**[**Kaspersky Small Office Security Management Console**](https://ksos.kaspersky.com/)**, and**[**Anti-Theft Web Management**](https://anti-theft.kaspersky.com/)**(hereinafter referred to as the "Service")**

**The categories of data**

**In order to use the Service and have access to all of its functions, you will provide following personal data:**

* your email address and password when you register on our Service;
* mobile phone number;
* information about your devices and licenses;
* information you provided to Kaspersky Lab’s technical support;
* expiration date of your bank card and the last 4 symbols of your bank card number;
* statistical information about your browser (domain names, IP addresses, network provider, browser types and other information about client environment, which Kaspersky Lab applications you use and how you use them, the web page you were visiting immediately prior to visiting our website, pages of our website that you visited, the time spent on those pages, information you searched for on our website, access times and dates, and other statistics from people who visit our site);
* full list of data collected on managed devices by My Kaspersky, please refer to section "[Conditions regarding data processing](https://my.kaspersky.com/Home/TermsOfUse)";
* full list of data collected on managed devices by Kaspersky Small Office Security Management Console, please refer to section "[Conditions regarding data processing](https://ksos.kaspersky.com/en/Home/TermsOfUse)".

**Description of Service**

***Account registration*. In order to use the Service and have access to all of its functions, you will need to create a personal account, which requires you to provide us with your email address (which will be your user name) and a password. We will only process and use this information in order to provide you the Service, unless you expressly opt in to a processing or use for other purposes (for example to receive useful news on Kaspersky Lab products and services via email). You may also need to provide us your mobile phone number for the purpose of additional protection of your account from unauthorized access. We will only use your mobile phone number to send you authorization security codes.**

***Account Settings and purchases*. You may review, update or correct your account data, password, and preferences or even delete your account at any time using the "Account Settings" function. Additionally, you will able to review your purchase history from our web store provider. In Account Settings, you are also able to link a bank card for easy purchases of additional Kaspersky Lab products and services. If you activate this option, our web store provider will attach your bank card data with your account and keep it for future orders. Kaspersky Lab will establish a special link to your web store provider account and will place orders on your behalf whenever they are performed by you. Our web store provider also gives us the information about expiration date of your bank card and the last 4 symbols of your bank card number. However, we will have no access to other data of your credit card stored by our web store provider. The linkage to your account will only be established technically by an internal User ID and password combination. These credentials will not grant us access to your bank card or other personal data stored by our web store provider. The internal User ID is used for triggering orders from you made through the web store.**

***Devices*. After registration, you will be able to manage all of your devices you secure using Kaspersky Lab products. You can, for example, secure lost or stolen devices, easily check the status of Kaspersky Lab products on each device or fix existing problems. To do that, you need to connect these devices using the "Devices" function. In that case, a link between your account and the devices you connect will necessarily be established. This will, of course, only be used for the purpose of providing you with the "Devices" function, unless you expressly opt in to a use it for other purposes.**

***Licenses*. You can manage all of your Kaspersky Lab product licenses using the "Licenses" function by adding your valid activation code(s) for each product and connect it to the device it is used on. You can also choose to be reminded of expiring licenses automatically or use the auto-renewal function. Reminders will only be sent to you by email if you expressly opt in to that.**

***Support*. If you request support from our Technical Support or Virus Lab team using support services, we will ask you for information needed to enable us to provide you with such support, such as your registration/ license number, the last 4 symbols of your bank card number used for purchasing the license, email address, and information about the product your problem relates to, your computer hardware, software and the nature of the problem you are experiencing. Furthermore, it may be helpful or even necessary for this purpose to send us files you are experiencing problems with via the "Upload" function. These may also contain personal information, such as user specific or otherwise personally identifiable file names, meta data or contents. It is, of course, always your choice whether you want to upload files or not. In case you do, please refer to our Regulation on Data Provisioning linked to the upload service and accept it at first.**

***Statistical information*.**We may track domain names, IP addresses, network provider, browser types and other information about client environment (such as model of your device, operating system, screen resolution, etc.) from people who visit our site. We may also process information about which Kaspersky Lab applications you use and how you use them, the web page you were visiting immediately prior to visiting our website, pages of our website that you visited, the time spent on those pages, information you searched for on our website, access times and dates, and other statistics. We use this information to produce traffic statistics for the Kaspersky Lab's sites and to improve security and availability of our websites and services. Such information is not correlated with any personal information. We do not ask you for, access or track any location based information from your device.

**How long do we keep your personal data**

Data is deleted no later than 1 (one) calendar month after the account is deleted.

**[Kaspersky Motorsport Website](https://www.kaspersky.com/about/sponsorships/)**

**The categories of data**

In order to use the Service and have access to all of its functions, you will provide following personal data:

* username and password;
* first name;
* last name;
* email address;
* your personal preferences;
* comments to other users.

**Description of Service**

***Connect With Us.***When you enter your details into this section of the website we will send you an email to confirm your subscription. Once confirmed we will regularly send you emails to keep you up to date with the latest news from Kaspersky Motorsport. You can change your details and unsubscribe at any point by using the relevant links that are contained within each email.

***Contact Us.***When you enter your details into this section of the website we will send you an email to confirm receipt of your query. We will only use your personal details from this form to reply to you about your query.

**How long do we keep your personal data**

You can delete your account at any point in time should you wish.  If you delete your account we will delete your personal information from our records within 24 hours.

**[Kaspersky Business Hub](https://cloud.kaspersky.com/)**

**The categories of data**

You must provide the following data to use Kaspersky Business Hub and gain access to all of its features:

* your personal account details:
  + email address and password;
  + security question to regain access to your account if you forget your password;
  + cellphone number;
  + country.
* information about your licenses for Kaspersky products that are available on Kaspersky Business Hub;
* statistical information about your device and web browser, which is collected when you visit our website;
* information given to Kaspersky technical support

**Description of Service**

***Account registration.***If you want to use Kaspersky Business Hub and have access to the products available in Kaspersky Business Hub, you need to create a personal account. To do this, you need to enter your email address (which will be used as your username) and a password. We will only process and use this information to provide you with Kaspersky Business Hub functionality and the products used in Kaspersky Business Hub. This information will only be processed and used for other purposes if you give your express consent (for example, to receive the latest news about Kaspersky products and services by email, or to be contacted about your Kaspersky product reviews). You can also provide your cellphone number to further protect your account from unauthorized access, as well as a security question to regain access to your account if you forget your password. We will only use your cellphone number to send security codes during your authorization.

You can view, update, and edit your account information or delete your account at any time by using the "Manage account" function.

***Licenses.***You can manage licenses for Kaspersky products that are available to you on Kaspersky Business Hub by using the "Licenses" function. To do this, you must add valid activation codes for each product that you use. We can send you an automatic license expiration reminder by email.

Access to managing certain licenses and using specific instances of our products depends on your access rights that are configured in the products.

We use the country that you specify when you register your account to provide the online license purchasing feature. Online sales of licenses are carried out by the online shop service provider (third party).

***Statistical information.***To collect comprehensive statistics on the use of Kaspersky Business Hub by website visitors, we may use various analytical services (third parties). You can find more information about our third-party policy in the "[DO WE USE COOKIES OR SOCIAL NETWORK MODULES](https://www.kaspersky.com/web-privacy-policy#Cookies)" section of this document. This information will be processed and used if you give your express consent when you visit Kaspersky Business Hub.

***Support.***When you contact Technical Support or the Virus Lab by using our support services, we will ask for the necessary information to provide you with support (for example, your license number, email address, information about the product that caused the problem, information about computer hardware and software, and a description of the problem). These files may also contain personal information, such as user or identifiable file names, metadata, or file content. You may send these files at your sole discretion.

**How long do we keep your personal data**

Your personal account information will be deleted no later than 1 (one) calendar month after the account is deleted. Backups of data are stored for no more than 1 (one) month from the moment when they are created.

**[Kaspersky Endpoint Security Cloud](https://cloud.kaspersky.com/)**

**The categories of data**

You must provide the following data to use Kaspersky Endpoint Security Cloud and gain access to all of its features:

* personal account details in Kaspersky Business Hub (you can see the relevant list of data and its processing policy in the section [Kaspersky Business Hub](https://www.kaspersky.com/web-privacy-policy#KBHub) of this document);
* data about your Kaspersky Endpoint Security Cloud workspaces:
  + information about your licenses for Kaspersky Endpoint Security Cloud;
  + data collected from the managed devices that are connected to the workspace;
* statistical information about your device and web browser, which is collected when you visit our website;
* information given to Kaspersky technical support.

**Description of Service**

***Account registration.***If you want to use Kaspersky Endpoint Security Cloud and have access to all of its features, you need to create a personal account on Kaspersky Business Hub. We undertake to process and use the email address that you provided during registration on Kaspersky Business Hub to provide you with Kaspersky Endpoint Security Cloud functionality. This information can only be processed and used for other purposes if you grant your express consent.

***Licenses.***You can manage licenses for Kaspersky Endpoint Security Cloud using the "Licenses" function. To do this, you must add valid activation codes for the licenses. We can send you an automatic license expiration reminder by email.

Access to managing specific licenses depends on your access rights, and on the access rights of other users of Kaspersky Business Hub. These access rights can be configured in the specific workspaces of Kaspersky Endpoint Security Cloud. For more information, please refer to our [online documentation](https://click.kaspersky.com/?hl=en-US&link=online_help&pid=Cloud&version=1.0&helpid=187780).

***Devices.***After creating a Kaspersky Endpoint Security Cloud workspace, you can manage the devices that are connected to your workspace and that are protected by Kaspersky products. Before you start managing your devices with Kaspersky Endpoint Security Cloud, you should take all necessary measures to comply with the relevant legislation concerning your use of Kaspersky Endpoint Security Cloud services. You should also change the Kaspersky Endpoint Security Cloud settings to reflect your usage. For more information, please refer to our [online documentation](https://click.kaspersky.com/?hl=en-US&link=online_help&pid=Cloud&version=1.0&helpid=187780). To ensure efficiency, devices managed in Kaspersky Endpoint Security Cloud transmit data to the administration servers located in the Kaspersky Endpoint Security Cloud infrastructure. The list of data collected from the managed devices is provided in the online documentation article "[About data provision](https://click.kaspersky.com/?hl=en-US&link=online_help&pid=Cloud&version=1.0&helpid=127176)."

***Statistical information.***To collect comprehensive statistics on the use of Kaspersky Endpoint Security Cloud by website visitors, we may use various analytical services (third parties). You can find more information about our third-party policy in the "[DO WE USE COOKIES OR SOCIAL NETWORK MODULES](https://www.kaspersky.com/web-privacy-policy#Cookies)" section of this document.

***Support.***When you contact Technical Support or the Virus Lab by using our support services, we will ask for the necessary information to provide you with support (for example, your license number, email address, information about the product that caused the problem, information about computer hardware and software, and a description of the problem). These files may also contain personal data, such as user or identifiable file names, metadata, and contents. You may send these files at your sole discretion.

**How long do we keep your personal data**

Data about your workspaces is deleted by using the "Managing Workspaces" function in Kaspersky Business Hub, or deleted automatically after your Kaspersky Endpoint Security Cloud license expires. Detailed information on the storage period for the data about workspaces can be found in the online documentation article "[About data provision](https://click.kaspersky.com/?hl=en-US&link=online_help&pid=Cloud&version=1.0&helpid=127176)."

**[Kaspersky Security Center Cloud Console](https://ksc.kaspersky.com/)**

**The categories of data**

You must provide the following data to use Kaspersky Security Center Cloud Console and gain access to all of its features:

* your personal account details:
  + email address and password;
  + security question to regain access to your account if you forget your password;
  + cellphone number;
* information about your licenses for the Kaspersky products that are available on Kaspersky Security Center Cloud Console;
* data about your Kaspersky Security Center Cloud Console workspaces:
  + information about your licenses for Kaspersky Security Center Cloud Console;
  + data collected from the managed devices that are connected to the workspace;
  + data that the user enters in the Kaspersky Security Center Cloud Console interface;
* statistical information about your device and web browser, which is collected when you visit our website;
* information given to Kaspersky technical support.

**Description of Service**

***Account registration.***If you want to use Kaspersky Security Center Cloud Console and have access to all of its features, you need to create a personal account on Kaspersky Security Center Cloud Console. To do this, enter your email address and password. We will only process and use this information to provide you with the Kaspersky Security Center Cloud Console functionality. This information can only be processed and used for other purposes if you grant your express consent. You can also provide your cellphone number to further protect your account from unauthorized access, as well as a security question to regain access to your account if you forget your password. We will only use your cellphone number to send security codes during your authorization.

You can view, update, and edit your account information or delete your account at any time by using the "Manage account" function.

***Licenses.***You can manage licenses for Kaspersky products that are available to you on Kaspersky Security Center Cloud Console by using the "Licenses" function. To do this, you must add valid activation codes for each product that you use. You can enable an automatic expiration reminder for the licenses that have been activated in Kaspersky products. Reminders will only be sent to you by email if you give your express consent.

***Devices.***After creating a Kaspersky Security Center Cloud Console workspace, you can manage devices that are connected to your workspace, and that are protected by Kaspersky products. Before you start managing your devices with Kaspersky Security Center Cloud Console, you should take all necessary measures to comply with the relevant legislation concerning your use of Kaspersky Security Center Cloud Console services. You should also change the Kaspersky Security Center Cloud Console settings to reflect your usage. For more information, please refer to our [online documentation](https://click.kaspersky.com/?hl=en-US&link=online_help&pid=ksc&version=1.0.0&helpid=5022). To ensure efficiency, devices managed in Kaspersky Security Center Cloud transmit data to the administration servers located in the Kaspersky Security Center Cloud infrastructure. The list of data collected from the managed devices is provided in the online documentation article "[About data provision](https://click.kaspersky.com/?hl=en&link=online_help&pid=ksc&version=1.0.0&helpid=175956)."

***Statistical information.***To collect comprehensive statistics on the use of Kaspersky Security Center Cloud by website visitors, we may use various analytical services (third parties). You can find more information about our third-party policy in the "[DO WE USE COOKIES OR SOCIAL NETWORK MODULES](https://www.kaspersky.com/web-privacy-policy#Cookies)" section of this document. If you give your express consent, this information will be processed and used when you visit Kaspersky Security Center Cloud Console.

***Support.***When you contact Technical Support or the Virus Lab by using our support services, we will ask for the necessary information to provide you with support (for example, your license number, email address, information about the product that caused the problem, information about computer hardware and software, and a description of the problem). These files may also contain personal information, such as user or identifiable file names, metadata, or file content. You may send these files at your sole discretion.

**How long do we keep your personal data**

Your personal account information will be deleted no later than 1 (one) calendar month after the account is deleted. Backups of data are stored for no more than 1 (one) month from the moment when they are created. Data about your workspaces is automatically deleted after your Kaspersky Security Center Cloud license expires or after you request its removal via Technical Support. After your license expires, you may be granted the right to continue using the Product, although the Product functionality may be limited. Detailed information on the storage period for the workspace data can be found in the online documentation article "[About data provision](https://click.kaspersky.com/?hl=en&link=online_help&pid=ksc&version=1.0.0&helpid=175956)."

**[Kaspersky Security for Microsoft Office 365](https://cloud.kaspersky.com/)**

**The categories of data**

In order to use the Service and have access to all of its functions, you will provide following personal data:

* email address;
* company name;
* password;
* your preferences;
* information you provided to Kaspersky Lab’s technical support;
* list of data that may be accessed by the Kaspersky Security for Microsoft Office 365 service as well as the data that is collected during operation of the service is presented in the documentation section "[About data provision](https://click.kaspersky.com/?link=online_help&hl=en-us&pid=KS365&version=1.2&helpid=144072)".

**Description of Service**

***Account registration.***In order to use Kaspersky Security for Microsoft Office 365 and have access to all of its functions, you will need to create a personal account, which requires you to provide us with your email address, company name, and password. You can use a Kaspersky Endpoint Security Cloud account. We will only process and use this information in order to provide you with the Kaspersky Security for Microsoft Office 365 service, unless you expressly opt in to processing or use for other purposes (for example, to receive useful news on Kaspersky Lab products and services via email). The email address specified during registration will be used for notifications related to provision of the Kaspersky Security for Microsoft Office 365 service, including to inform you when the service is unavailable, when the trial period expires, or when updates have been released.

***Account settings.***You may review, update or correct your account data, password and preferences or even delete your account any time using "Account Settings" function.

***Configuring the service.***The Kaspersky Security for Microsoft Office 365 service is integrated directly with Office 365, which requires access to Exchange Online or OneDrive. To configure your connection to Exchange Online or OneDrive, you will be redirected to the Microsoft Online website and prompted to grant permission for the Kaspersky Security for Office 365 application through the OAuth 2.0 flow. The Kaspersky Security for Microsoft Office 365 service also requires a Service Account to access Exchange Online quarantine. This Service Account can be configured automatically or manually. If you choose automatic configuration, the service asks you for Global Admin credentials. The Service does not save this data in any form, but instead uses it only for the initial configuration and creation of a Service Account. If you choose manual configuration, Global Admin credentials are not required, and the Service Account is created manually by the administrator.

***Service operation.***During operation, the Kaspersky Security for Microsoft Office 365 service receives messages and other objects (meetings, tasks, etc.) as well as OneDrive files to be scanned, and they are processed according to the protection settings. Kaspersky Security for Microsoft Office 365 does not save messages, OneDrive files, or objects requiring scanning in its infrastructure. The list of data that may be accessed by the Kaspersky Security for Microsoft Office 365 service as well as the data that is collected during operation of the service is presented in the documentation section "[About data provision](https://help.kaspersky.com/KS4MO365/1.2/en-US/144072.htm)".

***Support***. If you request support from our Technical Support or Virus Lab team using our technical support services, we will ask you for the information that we need in order to help you, such as your registration/license number, the last 4 symbols of your bank card number used for purchasing the license, email address, data of the product and service related to your problem, information about your computer hardware and software, and the nature of the problem you are experiencing. Furthermore, it may be helpful or even necessary for this purpose to send us files you are experiencing problems with via Company Account "upload" function. These may also contain personal information, such as user specific or otherwise personally identifiable file names, meta data or contents. It is of course always your choice whether you want to upload files or not.

**How long do we keep your personal data**

Data will be deleted after 6 months after your license expiration date.

**[Kaspersky CompanyAccount](https://companyaccount.kaspersky.com/)**

**The categories of data**

In order to use the Service and have access to all of its functions, you will provide following personal data:

* corporate email address (will be your username);
* password;
* your first name;
* your last name;
* company name;
* country;
* your company's license to use Kaspersky Lab applications;
* information you provided to Kaspersky Lab’s technical support. Please refer to section [Regulation on data provisioning](http://support.kaspersky.com/support/rdp?cid=ca&utm_source=companyaccount.kaspersky.com&utm_medium=referral&utm_campaign=company_account&utm_content=en).
* additional "third-party" email addresses (if added to the account).

**Description of Service**

***Account registration***. To use CompanyAccount and access all of its features, you must create:

* personal account;
* an account for your company, unless your coworkers have done this previously.

This will require that you provide your corporate email address (which will be your username), password, first and last name, company name and country, and your company's license to use Kaspersky Lab applications. We will process and use this information solely for the purpose of providing you with CompanyAccount services and technical support, unless you explicitly choose to have it processed and used for other purposes. After registration your personal account will be linked to your company's account. If your company's account was previously created, then your registration information (first and last name and corporate email address) will be sent to the CompanyAccount Administrator from your company. The company employee who first registers the company and a personal account is typically designated as the Administrator.

***Account settings.***You can at any time view, update, correct your account information and password, or delete your account on the "My account" tab. Your company's CompanyAccount Administrator will also be able to change your account settings and reset your password. If you are your company's CompanyAccount Administrator, then you have the ability to edit personal accounts for all of your colleagues and block the entire company's account (employees' personal accounts will remain in the system).

***Licenses***. You can add and view your company's licenses to Kaspersky Lab products on the "Licenses" tab of your CompanyAccount (activation codes or key files for each product). The license provided during registration will be added automatically to your company's CompanyAccount. Key files are not physically stored on CompanyAccount. The system only stores a record about your company's license. Every company employee with a personal account linked to your company's CompanyAccount has access to the list of licenses. Your CompanyAccount Administrator can remove your company's licenses by deleting them from the list.

***Contracts***. If your company purchases additional customer support services, then after the purchase has been recorded you will be able to view the list of purchases services on the "Contracts" tab. The list of contracts will be available to those company employees who were designated as authorized to use the paid service at the time of purchase. These people will automatically receive notifications about the expiration of the contract.

***Customer support requests.***If you contact Customer Support or the Anti-Virus Lab team for support through CompanyAccount, we may ask you to submit information we may require for providing assistance to you. For example, this may include information about the product associated with your request, computer hardware, your company's network, software, and the nature of the problem you've encountered. Moreover, it may be helpful or even necessary for you to send us the files you are having trouble with or files that define the configuration of your computer or network. You can do this by using the "Attach files" option in the request form. These files may contain user-specific or otherwise personally-identifiable file names, metadata, or content. It is always your choice whether to upload these files. If you would like to upload files, please first view and accept our [Regulation on data provisioning](http://support.kaspersky.com/support/rdp?cid=ca&utm_source=companyaccount.kaspersky.com&utm_medium=referral&utm_campaign=company_account&utm_content=en) on the file upload page. In order to choose the correct customer support department for your request, we will use information about your company's licenses, country, and possibly the interface language selected in your CompanyAccount. Your colleagues may have access to your requests if your CompanyAccount Administrator manually changes the corresponding settings (the Administrator can view requests automatically).

**How long do we keep your personal data**

You can delete your account at any time in the Account settings or by submitting a request to our Technical Support. Once your account has been deleted, your personal data will be held in Kaspersky Lab's database until the retention period has expired, but you will no longer be able to access the CompanyAccount website using the deleted account.

**[Kaspersky Lab Partner Portal](https://www.kasperskypartners.com/)**

**The categories of data**

In order to use the Service and have access to all of its functions, you will provide following personal data:

* email address;
* password;
* your name;
* address;
* phone number;
* information you provided to Kaspersky Lab’s technical support.

**Description of Service**

We may request personal information when you place an order, register a product, request a service, answer a survey, enter a contest, and when you correspond with us or engage in other activities on our website.

You make all decisions regarding whether or not to proceed with any activity that requests personal information. However, please note that if you do not wish to provide the requested information, you may not be able to complete the transaction.

We use personal information in the following ways:

* to provide you with information about virus alerts, product upgrades, new products, services, newsletters, informative emails, and research on future product ideas or improvements;
* to assist us in creating content that is relevant to you;
* to provide you with special Kaspersky-specific offers that may be of interest to you;
* to assist us in creating better products and services to meet your needs;
* to allow you to purchase and download products, obtain access to services, or otherwise engage in activities you select;
* to help you quickly find software, services or product information important to you.

Kaspersky Lab retains the services of outside vendors to provide services for us. They may be used to distribute products, provide technical support, or handle order processing. Our vendors are required to keep the personal information of customers secure and strictly confidential, and use personal information only on behalf of Kaspersky Lab and for no other purpose.

**How long do we keep your personal data**

Personal data stored all the time you use the service and will be deleted after your first request.

[**GSI Parser**](https://www.getsysteminfo.com/)

**The categories of data**

In order to use the Service and have access to all of its functions, you will provide following personal data:

* email address;
* password;
* report file (information about the hardware and software installed on the computer, the version of the operating system and installed service packs, kernel objects, drivers, services, Microsoft Internet Explorer add-ons, printing system extensions, Windows Explorer plug-ins, loaded objects, Active Setup items, control panel applets, records from the hosts file and system registry, versions of browsers and mail clients, information about established network connections and open ports at the moment when the information is submitted). Full list of provided information you can see in the section [Information provided](https://www.getsysteminfo.com/tou).

**Description of Service**

***General terms and conditions***. Kaspersky Lab hereby grants you the right to use the Website and to examine its Content for private use in order to ensure that the Kaspersky Lab Software is compatible with the other software installed on the Computer and/or drivers making up the Computer and to fix any bugs in the software. By uploading the report file to the Website, you acknowledge that you are the lawful owner of the uploaded object and that the object itself is not confidential and does not contain confidential information. By providing the object for analysis (uploading the object), you grant Kaspersky Lab a free-of-charge and exclusive license to copy, store and delete the uploaded object for analysis purposes. Data are transmitted to Kaspersky Lab via secure connections. The information provided will be protected by the Rights Holder in accordance with the requirements imposed by law and the requirements set out in the "Privacy Policy". The Website may not be used to create data, code or services for the purpose of detecting, blocking or removing viruses. Interfering with the operation of the Website or gaining access to the Website's services through circumvention of the standard interface (by means of undocumented routes) is prohibited. Use of the Website must comply with statutory regulations, including the applicable legislative instruments and export and re-export rules.

***User account creation.***You must create an account in order to use the website. To create your account, enter your email address and set a password.

***User account settings.***You can change your email address or password or permanently remove the account in the Manage Your Account section.

**How long do we keep your personal data**

The uploaded object will be stored on Kaspersky Lab's systems for no longer than 90 days, after which it will be deleted and cannot be restored.

**Other websites and forms**

**The categories of data**

In order to access various content elements, register for events, to test our products, to contact us by using our contact and support forms, prevent fraud, identity thefts and any other misuse of the Service, you will provide personal data that can include the following:

* first name;
* last name;
* email address;
* phone number;
* IP;
* UTC date.

**Description of Service**

***General terms and conditions***. Kaspersky Lab hereby grants you the right to use the Website and to view its Content for private use in order to ensure that the Kaspersky Lab Software is compatible.

***Premium Content.***In order to access various content elements, such as Whitepapers, Videos, register for events or reach dedicated marketing material, we will ask for your first name, last name, email and phone number as mandatory personal data to reach this premium content and to provide you with additional information on other content. These data will be used by our Kaspersky regional office responsible for your location to provide you with additional information on products, services, and other initiatives such as educational activities, seminars, events and marketing campaigns which might be of interest to you. The subscription is voluntary and you are free to unsubscribe anytime by clicking the unsubscribe link or contacting us by email address provided in the email message. In that case your registration data will be deleted and you will not be able to access Premium Content any longer, unless you subscribe for it again.

***Free trials.***If you want to test our products, we will also ask for your first name, last name, phone number and email address. This information will be used for sending out the activation code and to remind you of the end of the trial period. Up to 14 days after the end of the trial period you may receive a final reminder and an offer to purchase a full license. The trial registration is voluntary and you are free to withdraw your consent anytime by clicking the unsubscribe link or contacting us by email address provided in the email message. Upon your opt-out we will promptly delete your information unless you decide to purchase a full license.

***Newsletters, Free Product Updates and Special Offers.***If you have signed up for it and provided us your email address and, in some cases, your name and last name we will use these data to provide you with additional information on products and services free product updates and special offers which might be of interest to. The subscription is voluntary and you are free to unsubscribe anytime by clicking the unsubscribe link or contacting us by email address you will find in every email. In that case, your name and email address will be deleted and we will no longer send you these kinds of emails, unless you sign up again.

***Contact Forms.***If you want to contact us by using our contact and support forms, you will be asked to provide your contact information (entry fields marked “\*”), which we will exclusively process or use as far as necessary to get in contact with you and provide you with the information you desire. You are free to provide additional information (through the data fields not marked “\*”), which we will of course process in line with all applicable data protection requirements as well. This data will be forwarded to the Kaspersky regional teams responsible for your location. The Kaspersky regional teams will use the data in order to get in contact with you.

***Annual Customer Satisfaction Surveys for Technical Support users.***Kaspersky Lab holds per-incident surveys and an annual survey for Technical Support users with the purpose of improving the quality of service. In order to conduct the Annual Customer Satisfaction Surveys we receive the following information:

Your email address, which will allow us to identify you as a user in our database and link your opinion within the survey with your contacts and history of requests sent to our Technical Support Team.

The rate you gave to our Technical Support Team and recommendations that will be used for improving the quality of services provided by Kaspersky Lab Technical Support.

**How long do we keep your personal data**

Personal data stored all the time you use the service and will be deleted after your first request.

**DO WE USE COOKIES OR SOCIAL NETWORK MODULES**

Cookie files are files or fragments of information that may be saved on your computer or other Internet-compatible devices (for example, smartphones and tablets) when you visit our websites. This information frequently consists of alphanumeric strings that uniquely identify your computer, but they may also contain other information.

We use different types of “cookies” (small text files that are placed on your device):

* user input cookies;
* authentication cookies;
* cookies storing your preferences and settings;
* performance cookies;
* security (antifraud) cookies;
* third party advertising cookies;
* first party analytics cookies;
* social network tracking cookies.

We also use cookie files on our websites when you download Kaspersky Lab applications from our websites. This lets us improve user interaction with the website and product when you use Kaspersky Lab products and our websites and when you provide explicit consent.

Some of our web pages use electronic markers (web beacons) that we use to obtain comprehensive statistics regarding the effectiveness of our advertising campaigns and other operations. We also include web beacons in our emails to you in order to determine the effectiveness, performance, and optimization of email mailings and the user experience. We use various analytical services for these purposes. You can review a list of them [here](https://www.kaspersky.com/third-party-tracking).

You can configure your browser settings in a way that cookies are blocked or your system informs you whenever a website wants to set a cookie. However, please be aware that the blocking of cookies may have the effect that you will not be able to use all our website functions any more.

Also we use different types of “social plugins”. Please find here a [list of cookies embedded into our websites and table explaining how we use the social network modules.](https://www.kaspersky.com/third-party-tracking)

**KASPERSKY’S PRINCIPLES REGARDING DATA PROTECTION**

Our websites are principally designed in a way that limits the processing of personal data to a minimum. In certain cases we are obliged to transfer your personal data to third parties due to applicable legal requirements. This is for instance the case when there is reason to suspect a crime or misuse of our website.

For the provision of certain services we may make use of external service providers. As far as such external service providers need to have access to personal data, we ensure that any such access is limited to the extent necessary for the provision of the respective service. Furthermore, such external service providers of course have to submit themselves to comply with all applicable data protection regulations.

Our websites contain links to companies we maintain business relationships with, especially to our web shop providers. We are in no way responsible for compliance with data protection requirements regarding the use of our partner’s websites. For information concerning data protection when visiting theses websites, please refer to the respective companies’ website privacy policies.

**WHERE WE PROCESS INFORMATION**

The personal data provided by users to Kaspersky Lab can be processed in the countries, including countries outside the European Union (EU) or the European Economic Area (EEA) and can include the following: Germany, Netherlands, France, United Kingdom, Switzerland, Canada, Singapore, Russia, Japan, USA, Mexico, China, Azerbaijan. According to our general business practice, the data received from users in the EU is processed on servers located in the EU and Russia. Personal data may be processed at destinations outside the European Union (EU) or the European Economic Area (EEA) some of which have not been determined by the European Commission to have an adequate level of data protection. In which case Kaspersky Lab will transfer and disclose your data in compliance with the [European Commission’s adequacy decisions](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en) on certain countries and the Standard Contractual Clauses approved by the European Commission. You can request a copy of the Standard Contractual Clauses - please contact us at [click here](https://support.kaspersky.com/privacy).

Kaspersky Lab has taken appropriate security measures to protect your personal data in accordance with security and privacy best practices, including, utilizing the European Commission’s Standard Contractual Clauses for transfers of personal information between its group companies, which requires all group companies to protect personal information being processed from the European Economic Area to an equivalent standard to that required under European Union data protection law. Where we share your personal data with a third party service provider outside of the European Economic Area and Switzerland (as detailed in the section entitled “Recipients and legal basis for transfer”), we contractually oblige the third party service provider to implement adequate safeguards to protect your information.

**RECIPIENTS AND LEGAL BASIS FOR TRANSFER**

We never provide data, or access to data, to state organizations or third parties. We may only disclose information under restricted access as follows:

* Within the Kaspersky Lab group of companies. Your personal data will be used by our employees and other staff members on a need-to-know basis for the purposes described above.
* We also may share your information with vendors that help us in providing the services to us. These will process your personal data as data processors (Article 28 GDPR) solely on our behalf. The categories of such recipients include: provide web analytics, data processing, advertising, email distribution, payment processing, order fulfillment, and other services.

In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use the personal data they receive from us for any other purpose.

When we disclose your information to Group of Companies Kaspersky Lab and Service Providers outside the European Economic Area, we do so on the basis of the standards set out in the European Commission approved Standard Contractual Clauses for the export of personal data, and our own high standards of data security and respect for your privacy.

**YOUR RIGHTS AND YOUR PERSONAL DATA AND HOW TO EXERCISE THEM**

Also, we inform that you have certain rights regarding the personal data we store:

* **Right to be informed**. You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data, and your rights.
* **Right of access**. This enables you to receive a copy of the Personal Data we process about you and to check that we are lawfully processing it.
* **Right to rectification**. Request correction of the Personal Data that we process about you.
* **Right to erasure (Right to be forgotten)**. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it.
* **Right of restriction of processing**. This enables you to ask us to suspend the processing of Personal Data about you, for example if you want us to establish its accuracy or the reason for processing it.
* **Right to data portability**. Request the transfer of your Personal Data. We will provide to you, or a third party you have chosen, your Personal Data in a structured, commonly used, machine-readable format.
* **Right to object**. You may object at any time to our processing of your personal data when such processing is based on our legitimate interests.
* **Right to withdraw data protection consent**. If you withdraw your consent, we may not be able to provide you with access to the certain specific functionalities of our Site. We will advise you if this is the case at the time you withdraw your consent.
* **Right to complain**. You have the right to contact the data protection authority of your country in order to lodge a complaint against our data protection and privacy practices.
* **The right to deactivate cookies**. If you wish to restrict or block all the cookies which are set by our websites, please use the tool available on the particular website (if applicable), or refer to the Help function within your browser to learn how to manage your settings within your browser.

If you wish to exercise these rights, you may at any time directly [contact us](https://support.kaspersky.com/privacy).

Typically, you will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, except in relation to Consent Withdrawal, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive, or, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

**COMPLAINTS**

If you would like to make a complaint regarding this Privacy Policy or our practices in relation to your Personal Data, please contact us at [click here](https://support.kaspersky.com/privacy).

If you consider that the processing of personal data relating to you infringes applicable data protection law, you have the right to lodge a complaint with the competent supervisory authority at any time. Which supervisory authority has competence for your complaint can depend on the country where you reside.

Zeit Online

Formularbeginn

Formularende

**:Datenschutzerklärung**

16. September 2009, 13:09 UhrAktualisiert am 10. August 2020, 11:15 UhrQuelle: ZEIT ONLINE

Dies sind die Datenschutzbestimmungen der

**ZEIT Online GmbH**  
vertreten durch den Geschäftsführer Dr. Rainer Esser, Christian Röpke und Enrique Tarragona

Buceriusstraße, Eingang Speersort 1  
20095 Hamburg

Telefon: 040 / 32 80-0  
Fax: 040 / 32 71 11  
E-Mail: [email@zeit.de](mailto:email@zeit.de)

Der Schutz Ihrer Daten ist uns ein besonderes Anliegen, selbstverständlich beachten wir sämtliche für Deutschland geltende Datenschutzbestimmungen.

Im Folgenden informieren wir Sie im Einzelnen darüber, welche personenbezogenen Daten (also Daten, die einen Bezug zu Ihrer Person möglich machen, wie Name, Adresse oder aber auch IP-Adresse) wir auf unseren Internetseiten und im Zusammenhang mit den in dieser Datenschutzerklärungen genannten Diensten und Angeboten zu welchem Zweck erheben und wie lange diese Daten gespeichert werden. Darauffolgend informieren wir Sie ausführlich darüber, welche Rechte Ihnen in Bezug auf die Datenverarbeitung zustehen und wie Sie diese Rechte geltend machen.

Sollten Sie Fragen oder Anmerkungen zum Datenschutz auf unserer Internetseite haben, wenden Sie sich jederzeit gerne an uns. Eine entsprechende Kontaktaufnahme kann beispielsweise per E-Mail an [email@zeit.de](mailto:email@zeit.de) erfolgen.

**Übersicht:**

* [**TEIL I: Allgemeines**](https://www.zeit.de/hilfe/datenschutz#teil-i-allgemeines)
* [a.) zeit.de mit Werbung oder zeit.de Pur](https://www.zeit.de/hilfe/datenschutz#a-zeit-de-mit-werbung-oder-zeit-de-pur)
* [b.) Weitere Informationen zur Datenverarbeitung](https://www.zeit.de/hilfe/datenschutz#b-weitere-informationen-zur-datenverarbeitung)
* [c.) Gemeinsame Verantwortlichkeit der ZEIT Verlagsgruppe](https://www.zeit.de/hilfe/datenschutz#c-gemeinsame-verantwortlichkeit-der-zeit-verlagsgruppe)
* [d.) Datenübermittlung in Drittländer](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender)
* [**TEIL II: Technisch oder organisatorisch notwendige Daten**](https://www.zeit.de/hilfe/datenschutz#teil-ii-technisch-oder-organisatorisch-notwendige-daten)
* [a.) Abschluss eines Abonnements](https://www.zeit.de/hilfe/datenschutz#a-abschluss-eines-abonnements)
* [b.) Bestellungen im ZEIT-Shop](https://www.zeit.de/hilfe/datenschutz#b-bestellungen-im-zeit-shop)
* [c.) Registrierung Newsletter](https://www.zeit.de/hilfe/datenschutz#c-registrierung-newsletter)
* [d.) SSO-Account](https://www.zeit.de/hilfe/datenschutz#d-sso-account)
* [e.) Registrierung "graue Z+"](https://www.zeit.de/hilfe/datenschutz#e-registrierung-graue-z)
* [f.) Studiums-Interessentest](https://www.zeit.de/hilfe/datenschutz#f-studiums-interessentest)
* [g.) CHE Hochschulranking](https://www.zeit.de/hilfe/datenschutz#g-che-hochschulranking)
* [h.) ZEIT-Stellenmarkt](https://www.zeit.de/hilfe/datenschutz#h-zeit-stellenmarkt)
* [i.) Kontaktaufnahme](https://www.zeit.de/hilfe/datenschutz#i-kontaktaufnahme)
* [j.) Kommentierung von Beiträgen / Forennutzung und Blog](https://www.zeit.de/hilfe/datenschutz#j-kommentierung-von-beitraegen-forennutzung-und-blog)
* [k.) ZEIT Akademie](https://www.zeit.de/hilfe/datenschutz#k-zeit-akademie)
* [l.) ZEIT Reisen](https://www.zeit.de/hilfe/datenschutz#l-zeit-reisen)
* [m.) Freunde der ZEIT](https://www.zeit.de/hilfe/datenschutz#m-freunde-der-zeit)
* [n.) Nutzung Ihrer Daten zu Werbezwecken](https://www.zeit.de/hilfe/datenschutz#n-nutzung-ihrer-daten-zu-werbezwecken)
* [o.) ZEIT Campus Berufsorientierungsangebot (BOA)](https://www.zeit.de/hilfe/datenschutz#o-zeit-campus-berufsorientierungsangebot-boa)
* [p.) ZEIT Umfragen und ZEIT Gewinnspiele](https://www.zeit.de/hilfe/datenschutz#p-zeit-umfragen-und-zeit-gewinnspiele)
* [q.) ZEIT Audio Skill](https://www.zeit.de/hilfe/datenschutz#q-zeit-audio-skill)
* [r.) Podigee Podcast-Hosting](https://www.zeit.de/hilfe/datenschutz#r-podigee-podcast-hosting)
* [**TEIL III: Bei der Nutzung unserer Website automatisch erhobene Daten**](https://www.zeit.de/hilfe/datenschutz#teil-iii-bei-der-nutzung-unserer-website-automatisch-erhobene-daten)
* [a.) Logfiles](https://www.zeit.de/hilfe/datenschutz#a-logfiles)
* [b.) iq digital Werbungsvermarktung](https://www.zeit.de/hilfe/datenschutz#b-iq-digital-werbungsvermarktung)
* [c.) Messverfahren ("SZMnG") der INFOnline GmbH](https://www.zeit.de/hilfe/datenschutz#c-messverfahren-szmng-der-infonline-gmbh)
* [d.) Webtrekk GmbH](https://www.zeit.de/hilfe/datenschutz#d-webtrekk-gmbh)
* [e.) Meetrics GmbH](https://www.zeit.de/hilfe/datenschutz#e-meetrics-gmbh)
* [h.)  Facebook](https://www.zeit.de/hilfe/datenschutz#h-facebook)
* [i.) CeleraOne](https://www.zeit.de/hilfe/datenschutz#i-celeraone)
* [j.) Google](https://www.zeit.de/hilfe/datenschutz#j-google)
* [k.) Adtriba](https://www.zeit.de/hilfe/datenschutz#k-adtriba)
* [l.) YouTube](https://www.zeit.de/hilfe/datenschutz#l-youtube)
* [m.) Brightcove](https://www.zeit.de/hilfe/datenschutz#m-brightcove)
* [n.) Outbrain (ehemalig Ligatus)](https://www.zeit.de/hilfe/datenschutz#n-outbrain-ehemalig-ligatus)
* [o.) emetriq](https://www.zeit.de/hilfe/datenschutz#o-emetriq)
* [p.) Moat](https://www.zeit.de/hilfe/datenschutz#p-moat)
* [q.) Yieldlab](https://www.zeit.de/hilfe/datenschutz#q-yieldlab)
* [r.) MaxMind](https://www.zeit.de/hilfe/datenschutz#r-maxmind)
* [s.) Tealium](https://www.zeit.de/hilfe/datenschutz#s-tealium)
* [t.) Twitter](https://www.zeit.de/hilfe/datenschutz#t-twitter)
* [u.) Typeform](https://www.zeit.de/hilfe/datenschutz#u-typeform)
* [v.) Linkpulse](https://www.zeit.de/hilfe/datenschutz#v-linkpulse)
* [**TEIL IV: Ihre Rechte**](https://www.zeit.de/hilfe/datenschutz#teil-iv-ihre-rechte)
* [a.) Recht auf Auskunft](https://www.zeit.de/hilfe/datenschutz#a-recht-auf-auskunft)
* [b.) Recht auf Berichtigung](https://www.zeit.de/hilfe/datenschutz#b-recht-auf-berichtigung)
* [c.) Recht auf Löschung](https://www.zeit.de/hilfe/datenschutz#c-recht-auf-loeschung)
* [d.) Recht auf Einschränkung](https://www.zeit.de/hilfe/datenschutz#d-recht-auf-einschraenkung)
* [e.) Recht auf Übermittlung](https://www.zeit.de/hilfe/datenschutz#e-recht-auf-uebermittlung)
* [f.) Recht auf Widerspruch](https://www.zeit.de/hilfe/datenschutz#f-recht-auf-widerspruch)
* [g.) Recht auf Beschwerde bei der Aufsichtsbehörde](https://www.zeit.de/hilfe/datenschutz#g-recht-auf-beschwerde-bei-der-aufsichtsbehoerde)
* [**TEIL V: Gemeinsame Verantwortlichkeit**](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit)

[Mehr anzeigen](https://www.zeit.de/hilfe/datenschutz#flexible-toc)

**TEIL I: Allgemeines**

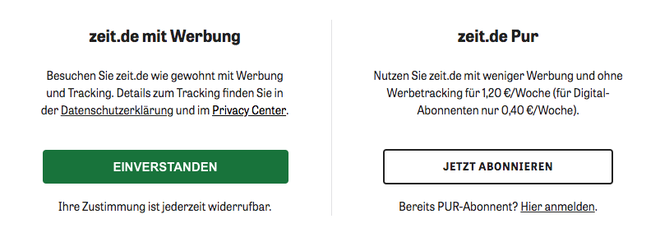
Auf unseren Internetseiten erheben wir Daten verschiedener Art. So erheben wir zum einen Daten, die Sie freiwillig eintragen, beispielsweise wenn Sie ein Abonnement oder etwas in unserem ZEIT Shop bestellen, einen unserer zahlreichen Newsletter abonnieren oder Kontakt zu uns aufnehmen, eine Befragung ausfüllen, sich an unseren Diskussionsforen beteiligen, an einem Wettbewerb teilnehmen oder ähnliche Dienste in Anspruch nehmen.

Zum anderen erheben wir über auf unseren Internetseiten eingesetzte Cookies bzw. Pixel Informationen und allgemeine Daten über die Nutzung unserer Internetseite, die automatisch bei der Nutzung unserer Internetseite an uns, bzw. an Dritte übermittelt werden.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#teil-i-allgemeines)

**a.) zeit.de mit Werbung oder zeit.de Pur**

Das Angebot von zeit.de können Sie entweder über einen kostenlosen, ausschließlich werbefinanzierten Zugang oder über einen kostenpflichtigen Zugang ohne Werbetracking mit deutlich reduzierter Werbung ("Pur-Abo") nutzen. Bevor unsere eigentliche Webseite geladen wird, können Sie sich aktiv für eine der beiden Optionen entscheiden.

[](https://www.zeit.de/zustimmung)

Nur wenn Sie sich aktiv für den kostenlosen Zugang entschieden haben, speichern und nutzen wir Cookies, Geräte-IDs und ähnliche Tracking-Technologien auf Endgeräten, um die Erhebung von Nutzungsdaten und deren pseudonymisierte Verarbeitung zu Nutzungsprofilen zum Zwecke einer nutzungsbasierten Werbeausspielung zu ermöglichen ("Werbetracking"). Dies geschieht, weil wir in diesem Fall unser Angebot mit Ihrer Einwilligung durch weitere, mittels Werbetracking optimierte Werbung finanzieren. Rechtsgrundlage der Datenverarbeitung ist dann Art. 6 Abs. 1 lit. a DSGVO

Unabhängig von Ihrer Zustimmung zum Werbetracking werden jedoch auch im Pur-Abo weiterhin essentielle sowie für interne/allgemeine Nutzungsanalysen notwendige Cookies und Tracking-Technologien, insbesondere zur Reichweitenmessung und Funktionssicherung, genutzt. Hieran haben wir ein überwiegendes berechtigtes Interesse, Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#a-zeit-de-mit-werbung-oder-zeit-de-pur)

**b.) Weitere Informationen zur Datenverarbeitung**

Weitere Informationen zur Datenverarbeitung im Pur-Abo finden Sie unter Teil [II a)](https://www.zeit.de/hilfe/datenschutz#a-abschluss-eines-abonnements), weitere Informationen zur Datenverarbeitung im kostenlosen Zugang sowie zur Widerrufsmöglichkeit Ihrer Einwilligung zum Werbetracking unter [Teil III](https://www.zeit.de/hilfe/datenschutz#teil-iii-bei-der-nutzung-unserer-website-automatisch-erhobene-daten).

Die Datenverarbeitungen sind im Einzelnen in den Teilen [III](https://www.zeit.de/hilfe/datenschutz#teil-iii-bei-der-nutzung-unserer-website-automatisch-erhobene-daten). und [IV](https://www.zeit.de/hilfe/datenschutz#teil-iv-ihre-rechte). beschrieben. In [Teil IV](https://www.zeit.de/hilfe/datenschutz#teil-iv-ihre-rechte). erfahren Sie, welche Rechte Ihnen im Zusammenhang mit der Verarbeitung Ihrer Daten zustehen.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#b-weitere-informationen-zur-datenverarbeitung)

**c.) Gemeinsame Verantwortlichkeit der ZEIT Verlagsgruppe**

Soweit Ihre Daten in gemeinsamer Verantwortlichkeit innerhalb der ZEIT Verlagsgruppe oder Dritter verarbeitet werden ("Joint-Controllership", Art 26 DSGVO), werden Sie hierüber in den unten folgenden Beschreibungen der einzelnen Datenverarbeitungen informiert. Eine Übersicht, welche Unternehmen der ZEIT Verlagsgruppe an welchen Verarbeitungen wie beteiligt sind, finden Sie außerdem im Abschnitt [TEIL V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

Über ihr JointControllership haben die Verantwortlichen eine Vereinbarung gemäß Art. 26 Abs. 1 DSGVO geschlossen. Weitere Informationen zur gemeinsamen Verantwortlichkeit insbesondere zu den Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen erteilen wir Ihnen gerne auf Anfrage.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#c-gemeinsame-verantwortlichkeit-der-zeit-verlagsgruppe)

**d.) Datenübermittlung in Drittländer**

Der Besuch unserer Website, sowie die Nutzung unserer Services kann mit der Übermittlung bestimmter personenbezogener Daten in Drittländer, also Länder, in denen die DSGVO nicht geltendes Recht ist, verbunden sein. Eine solche Übermittlung erfolgt in zulässiger Weise, wenn die Europäische Kommission festgestellt hat, dass in dem Drittland ein angemessenes Datenschutzniveau geboten ist. Wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, erfolgt eine Übermittlung personenbezogener Daten in ein Drittland nur beim Vorliegen geeigneter Garantien gem. Art. 46 DSGVO oder wenn eine der Voraussetzungen des Art. 49 DSGVO gegeben ist.

Sofern im Folgenden nichts anderes angegeben ist, verwenden wir als geeigneten Garantien die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087>.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender)

**TEIL II: Technisch oder organisatorisch notwendige Daten**

Die Nutzung unserer Internetseiten ist regelmäßig ohne Eingabe von personenbezogenen Daten möglich. Lediglich in einigen wenigen, im Folgenden einzeln aufgelisteten Fällen, ist eine freiwillige Angabe von personenbezogenen Daten jedoch notwendig, da wir Ihnen unsere Dienste sonst nicht zur Verfügung stellen können. Die Daten verwenden wir zu den nachfolgend im einzelnen genannten Zwecken.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#teil-ii-technisch-oder-organisatorisch-notwendige-daten)

**a.) Abschluss eines Abonnements**

Schließen Sie über unsere Internetseite ein [Abonnement der Zeitung](https://abo.zeit.de/) "DIE ZEIT", ein Abonnement für eines der ZEIT Magazine der Zeitverlag Gerd Bucerius GmbH & Co. KG, ein Abonnement der [digitalen Ausgabe der ZEIT](https://premium.zeit.de/) oder der Magazine und/oder ein Pur-Abo ab, so ist hierfür die Angabe der folgenden Daten notwendig: Vorname, Name, Adresse, E-Mail. Ihre Telefonnummer können Sie freiwillig eintragen, diese ist zur Vertragsbegründung nicht notwendig. Ihre Bankdaten benötigen wir dann, wenn Sie eine Zahlung im Lastschriftverfahren wünschen, andernfalls ist auch diese zur Vertragsbegründung nicht notwendig.

Die genannten Daten benötigen wir, um unsere Verpflichtungen aus dem geschlossenen Abonnementvertrag zu erfüllen, Art. 6 Abs. 1 lit. b) DSGVO.

Schließen Sie ein Abonnement der Zeitung DIE ZEIT ab, so geben wir Ihre Daten zum Zwecke der Abwicklung des Abonnements weiter an die DPV Deutscher Pressevertrieb GmbH, Am Baumwall 11, 20459 Hamburg. Die Datenweitergabe ist zur Vertragserfüllung erforderlich und beruht insoweit auf Art. 6 Abs. 1 lit. b) DSGVO.

Abonnieren Sie die digitale Ausgabe der ZEIT, ist es hierfür notwendig, dass Sie auf unserer Internetseite [meine.zeit.de](http://meine.zeit.de/)einen [SSO-Account](https://www.zeit.de/hilfe/datenschutz#d-sso-account) erstellen. In diesem Zusammenhang müssen Sie Ihre E-Mailadresse angeben. Die Angabe dieser Daten ist zur Vertragserfüllung erforderlich, ihre Verarbeitung beruht auf Art. 6 Abs. 1 lit. b) DSGVO.

Wir speichern Ihre Daten zunächst bis zum Ende Ihres Abonnements und danach bis zum Ablauf der gesetzlichen Verjährungsfrist. An der diesbezüglichen Speicherung Ihrer Daten haben wir ein berechtigtes Interesse, welches sich bereits aus Art. 17 Abs. 3 lit. e) DSGVO ergibt. Die Speicherung Ihrer Daten beruht insoweit auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Darüber hinaus speichern wir gemäß Art. 6 Abs. 1 lit c) DSGVO personenbezogene Daten zur Erfüllung unserer gesetzlichen Aufbewahrungspflichten nach § 257 Abs. 4 HGB, § 147 Abs. 3 AO. Dies betrifft z.B. Eintragungen im Kontokorrentbuch, Buchungsbelege und Rechnungen zu Ihrem Abonnement. Die Aufbewahrungsfrist beträgt maximal zehn Jahre und beginnt mit dem Schluss des Kalenderjahres, in dem die letzte Eintragung in das Buch gemacht oder der Buchungsbeleg entstanden ist, ferner die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind.

Wenn Sie ein Probe-Abonnement abschließen und später kündigen, speichern wir Ihre Daten für die Dauer eines Jahres nach der Kündigung eines Probe-Abonnements, um sicherzustellen bzw. überprüfen  zu können, dass sich eine Person in diesem Zeitraum nicht mehrfach für ein kostenloses Probeabonnement anmeldet. Einen entsprechenden Ausschluss von Mehrfachanmeldungen behalten wir uns in unseren AGB ausdrücklich vor. Die entsprechende Datenverarbeitung beruht auf dem, sich aus diesen Gründen ergebenden berechtigtem Interesse und damit auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Die Datenverarbeitung im Rahmen von Abonnementverwaltung und Vertrieb findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#a-abschluss-eines-abonnements)

**b.) Bestellungen im ZEIT-Shop**

Kaufen Sie in unserem [ZEIT-Shop](https://shop.zeit.de/) ein, ist zur Vertragserfüllung die Angabe der folgenden Daten notwendig: Vorname, Name, Adresse, E-Mail. Ihre Telefonnummer können Sie freiwillig eintragen, diese ist zur Vertragsbegründung nicht notwendig. Ihre Bankdaten benötigen wir dann, wenn Sie eine Zahlung im Lastschriftverfahren wünschen, andernfalls ist auch diese zur Vertragsbegründung nicht notwendig. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b) DSGVO.

Bestellen Sie ein Produkt über den ZEIT Shop, so geben wir Ihre Daten zum Zwecke der Abwicklung der Bestellung weiter an die Sigloch Distribution GmbH & Co. KG, Am Buchberg 8, 74572 Blaufelden.

Bestellen Sie ein Einzelheft bei uns im Shop, so geben wir Ihre Daten zum Zwecke der Abwicklung der Bestellung weiter an die DPV Deutscher Pressevertrieb GmbH, Am Baumwall 11, 20459 Hamburg.

Zudem werden Ihre Daten an etwaige mit der Zahlungsabwicklung beauftragte Kreditinstitute oder im Falle der Auswahl einer Zahlung über Paypal an die PayPal (Europe) S.à r.l. et Cie, S.C.A.22-24 Boulevard Royal, L-2449 Luxembourg weitergegeben. Die Datenweitergabe dient der Vertragserfüllung und beruht insoweit auf Art. 6 Abs. 1 lit. b) DSGVO.

Ihre persönlichen Daten werden zu den genannten Zwecken bis zum Ende der Abwicklung des bestehenden Vertrages verarbeitet. Darüber hinaus speichern wir gemäß Art. 6 Abs. 1 lit c) DSGVO personenbezogene Daten zur Erfüllung unserer gesetzlichen Aufbewahrungspflichten nach § 257 Abs. 4 HGB, § 147 Abs. 3 AO. Dies betrifft z.B. Eintragungen im Kontokorrentbuch, Buchungsbelege und Rechnungen zu Ihrer Bestellung. Die Aufbewahrungsfrist beträgt maximal zehn Jahre und beginnt mit dem Schluss des Kalenderjahres, in dem die letzte Eintragung in das Buch gemacht oder der Buchungsbeleg entstanden ist, ferner die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind. Im Anschluss werden Ihre Daten gelöscht.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#b-bestellungen-im-zeit-shop)

**c.) Registrierung Newsletter**

Sie haben auf unseren [Internetseiten](https://community.zeit.de/newsletter) die Möglichkeit sich für unsere/n Newsletter zu registrieren. Hierfür ist es notwendig, dass Sie uns Ihre E-Mailadresse sowie Ihren Vor- und Nachnamen mitteilen. Diese Angaben sind für die Eintragung in die Versandliste notwendig. Ihre Anschrift können Sie freiwillig angeben.

Die genannten Daten benötigen wir, um Ihnen den Newsletter zusenden zu können. Die entsprechende Verarbeitung Ihrer Daten  beruht auf der von Ihnen entsprechend erteilten Einwilligung und damit auf Art. 6 Abs. 1 lit. a) DSGVO.

Registrieren Sie sich für unseren Newsletter, so geben wir Ihre Daten zum Zwecke der Abwicklung weiter an die Episerver GmbH, Wallstr. 16, 10179 Berlin sowie an die  Mailjet GmbH, Berliner Allee 26, 40212 Düsseldorf.

Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. f) DSGVO

Ihre Einwilligung in die Zusendung des Newsletters können Sie jederzeit, beispielsweise via E-Mail an [email@zeit.de](mailto:diezeit@zeit.de) widerrufen. Eine Abmeldung vom Newsletter ist zudem jederzeit durch einen Klick auf den in jedem Newsletter enthaltenen Abmelde-Link möglich.

Wir speichern Ihre Daten zu diesem Zweck solange uns kein Widerruf Ihrer Einwilligung oder ein Widerspruch gegen die Verarbeitung Ihrer Daten zu Werbezwecken vorliegt.

**Newslettererfolgsmessung:**  
Die Newsletter enthalten einen sog. "web-beacon", d.h. eine pixelgroße Datei, die beim Öffnen des Newsletters von unserem Server, bzw. sofern wir einen Versanddienstleister einsetzen, von dessen Server abgerufen wird. Im Rahmen dieses Abrufs werden zunächst technische Informationen, wie Informationen zum Browser und Ihrem System, als auch Ihre IP-Adresse und Zeitpunkt des Abrufs erhoben.

Diese Informationen werden zur technischen Verbesserung der Services anhand der technischen Daten oder der Zielgruppen und ihres Leseverhaltens anhand derer Abruforte (die mit Hilfe der IP-Adresse bestimmbar sind) oder der Zugriffszeiten genutzt. Zu den statistischen Erhebungen gehört ebenfalls die Feststellung, ob die Newsletter geöffnet werden, wann sie geöffnet werden und welche Links geklickt werden. Diese Informationen können aus technischen Gründen zwar den einzelnen Newsletterempfängern zugeordnet werden. Es ist jedoch weder unser Bestreben, noch, sofern eingesetzt, das des Versanddienstleisters, einzelne Nutzer zu beobachten. Die Auswertungen dienen uns viel mehr dazu, die Lesegewohnheiten unserer Nutzer zu erkennen und unsere Inhalte auf sie anzupassen oder unterschiedliche Inhalte entsprechend den Interessen unserer Nutzer zu versenden. Rechtsgrundlage der Datenverarbeitung zur Newslettererfolgsmessung ist somit Art. 6 Abs. 1 lit. f) DSGVO

Ein getrennter Widerruf der Erfolgsmessung ist in jedem Newsletter per Klick auf dem im Footer angegebenen Link "Um den Personenbezug des Trackings zu deaktivieren, klicken Sie bitte hier" möglich.

Die Datenverarbeitung im Rahmen des Newsletters und der Newslettererfolgsmessung findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#c-registrierung-newsletter)

**d.) SSO-Account**

Auf unserer [Internetseite](http://meine.zeit.de/) bieten wir Ihnen die Möglichkeit, sich unter Angabe Ihrer E-Mailadresse einen SSO-Account anzulegen. Dieser Account ist Grundlage verschiedener unserer registrierungspflichtiger Dienste.

Als registrierter Nutzer stehen Ihnen neben verschiedenen Diensten wie den Berufsorientierungsangeboten, Z+, SIT, CHE, BOA zudem die folgenden Dienste zur Verfügung:

* Sie können Kommentare zu Artikeln auf ZEIT Online sowie eigene Leserartikel verfassen, um sich mit der Redaktion sowie mit anderen Nutzern auszutauschen. Kommentare sind kürzere Textbeiträge, die Sie unter vorhandenen Artikeln, Videos, Fotostrecken oder anderen Multimedia-Inhalten abgeben können. Leserartikel sind von Ihnen verfasste Texte, die wir nach vorheriger Auswahl, Prüfung und eventuell redaktioneller Bearbeitung auf ZEIT ONLINE veröffentlichen. Durch Ihre Beiträge wollen wir die Inhalte um spannende Perspektiven und lebendige Diskussionen ergänzen.
* Zudem können Sie als registrierter Nutzer jede Woche eine Auswahl registrierungspflichtiger Inhalte lesen (markiert mit einem grauen Z+),
* bei unserem Wissensquiz Ihren Spielstand speichern, eigene Quizze erstellen und das ZEIT ONLINE Schach spielen.

Für die Erstellung eines entsprechenden Accounts ist ausschließlich die Angabe Ihrer E-Mailadresse erforderlich. Im Zeitpunkt der Registrierung werden zudem Ihre IP-Adresse sowie Datum und Uhrzeit der Registrierung gespeichert. Nach der Registrierung erhalten Sie dann eine bestätigende E-Mail von uns, mit welcher Sie Ihre Registrierung abschließen können. Zum Abschluss der Registrierung ist die Angabe eines Passwortes notwendig, welches wir speichern.

Die Angabe der E-Mailadresse und des Passwortes sind für die Registrierung notwendig. Als registrierter Nutzer haben Sie die Möglichkeit auf verschiedene Angebote zuzugreifen und entsprechende Such- oder Nutzungsprofile zu erstellen. Weitere Informationen hierzu finden Sie in der Beschreibung der jeweiligen Dienste.

Die Verarbeitung Ihrer Daten ist zur Registrierung erforderlich und beruht auf Art. 6 Abs. 1 lit. b) DSGVO und darüber hinaus auf der von Ihnen entsprechend erteilten Einwilligung und damit auf Art. 6 Abs. 1 lit. a) DSGVO.

Ihre Daten werden zu diesem Zweck für die Dauer Ihrer bestehenden Registrierung gespeichert.

Bitte beachten Sie, dass bei Anmeldung zu Ihrem Account im Browser Ihres Endgeräts ein sogenannter SSO-Cookie bis zu einem Jahr gespeichert wird. Dieser Cookie bleibt dort auch nach Löschung Ihres Accounts gespeichert. Um den Löschvorgang abzuschließen, melden Sie sich daher bitte auf allen Ihren Endgeräten von Ihrem Account ab. Nutzen Sie hierzu bitte den Link meine.zeit.de/abmelden. Mit der Abmeldung wird der SSO-Cookie in Ihrem Browser gelöscht und der gesamte Löschvorgang damit abgeschlossen.

Die Datenverarbeitung im Rahmen Ihres SSO-Accounts findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#d-sso-account)

**e.) Registrierung "graue Z+"**

Auf unserer Internetseite bieten wir Ihnen die Möglichkeit, sich unter Angabe Ihrer E-Mailadresse für unseren Dienst "graue Z+" zu registrieren. Mit der Registrierung für Z+ ist es Ihnen möglich, eine Auswahl der registrierpflichtigen Artikel online zu lesen. Hierfür ist es notwendig, dass Sie sich kostenfrei unter Angabe Ihrer E-Mailadresse registrieren. Im Zeitpunkt der Registrierung über den SSO-Account werden zudem Ihre IP-Adresse sowie Datum und Uhrzeit der Registrierung gespeichert. Weitere Infos zur Verarbeitung der Daten in dem Zusammenhang mit der Erstellung des SSO-Accounts finden Sie unter der entsprechenden Überschrift ["SSO-Account"](https://www.zeit.de/hilfe/datenschutz#d-sso-account).

Nach der Registrierung erhalten Sie eine bestätigende E-Mail von uns, mit welcher Sie Ihre Registrierung abschließen können. Zum Abschluss der Registrierung ist die Angabe eines Passwortes notwendig, welches wir verschlüsselt speichern. Zudem speichern wir nach entsprechender Angabe Ihr Suchprofil , sowie weitere persönliche Daten, sofern Sie diese angeben, wie Anrede, Titel Name und Vorname. Die Angabe der E-Mailadresse und des Passwortes sind für die Registrierung notwendig. Die Angabe aller weiteren Daten ist freiwillig. Die Verarbeitung Ihrer Daten beruht soweit sie zur Erfüllung des Vertrags notwendig ist auf Art. 6 Abs. 1 lit. b) DSGVO und darüber hinaus auf der von Ihnen entsprechend erteilten Einwilligung und Art. 6 Abs. 1 lit. a) DSGVO.

Ihre Daten werden zu diesem Zweck für die Dauer Ihrer bestehenden Registrierung gespeichert.  
Die Datenverarbeitung im Rahmen Ihres SSO-Accounts findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://vivi.zeit.de/workingcopy/ldap.ehlers/datenschutz-2/@@edit.html#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#e-registrierung-graue-z)

**f.) Studiums-Interessentest**

Sie haben die Möglichkeit auf unserer [Seite](https://studiengaenge.zeit.de/sit) den "Studium-Interessentest" (SIT) zu absolvieren. Damit Sie an dem SIT teilnehmen können, ist es notwendig, dass Sie zunächst einen SSO-Account anlegen und sich unter Angabe Ihrer E-Mailadresse registrieren. Weitere Infos zur Verarbeitung der Daten in dem Zusammenhang mit der Erstellung des SSO-Accounts finden Sie unter der entsprechenden Überschrift ["SSO-Account"](https://www.zeit.de/hilfe/datenschutz#d-sso-account). In einem zweiten Schritt werden Ihnen dann verschiedene Fragen gestellt, deren Beantwortung nötig ist, um den Test auszuwerten.

Die von Ihnen angegebenen Daten sind zur Auswertung des Testes und der Übersendung des Ergebnisses notwendig. Die Datenverarbeitung beruht insoweit auf Art. 6 Abs. 1 lit. b) DSGVO.

Der SIT ist Teil der Angebote zur Studien- und Berufsorientierung (BOA, Studium-Interessentest, Suchmaschine für Studiengänge und CHE-Ranking). Im Rahmen dieser haben Sie die Möglichkeit z.B. ein eigenes Nutzerprofil zu erstellen und Dienste wie Merklisten, Testergebnisse und personalisierte Trefferlisten zu nutzen.

Es findet eine Weiterleitung von anonymisierten Daten an die Cyquest GmbH, Heußweg 25, 20255 Hamburg zu Auswertungszwecken der SIT Antworten statt. Es besteht für die Cyquest GmbH keine Möglichkeit einen Personenbezug herzustellen. Die Weiterleitung ist zur Vertragserfüllung erforderlich und beruht auf Artikel 6 Abs. 1 lit. b) DSVGO.

Wir speichern Ihre personenbezogenen Daten zu diesen Zwecken für die Dauer des Bestehen Ihres Accounts.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#f-studiums-interessentest)

**g.) CHE Hochschulranking**

Auf unserer [Internetseite](https://ranking.zeit.de/che/de/) haben Sie die Möglichkeit, die Ergebnisse des aktuellen CHE-Hochschulrankings einzusehen. Hierfür ist es notwendig, dass Sie zunächst einen SSO-Account anlegen und sich unter Angabe Ihrer E-Mailadresse registrieren. Weitere Infos zur Verarbeitung der Daten in dem Zusammenhang mit der Erstellung des SSO-Accounts finden Sie unter der entsprechenden Überschrift ["SSO-Account"](https://www.zeit.de/hilfe/datenschutz#d-sso-account).

Die Angabe der E-Mailadresse ist zur Vertragserfüllung erforderlich. Die Verarbeitung der Daten beruht auf Artikel 6 Abs. 1 lit. b) DSVGO. Die Verarbeitung aller im Weiteren freiwillig angegebenen Daten beruht auf Ihrer entsprechenden Einwilligung und damit auf Art. 6 Abs. 1 lit. a) DSGVO.

Der CHE ist Teil der Angebote zur Studien- und Berufsorientierung (BOA, Studium-Interessentest, Suchmaschine für Studiengänge und CHE-Ranking). Im Rahmen dieser haben Sie die Möglichkeit z.B. ein eigenes Nutzerprofil zu erstellen und Dienste wie Merklisten, Testergebnisse und personalisierte Trefferlisten zu nutzen.

Die Erfassung der Daten wird von ZEIT ONLINE in Zusammenarbeit mit den Dienstleistern Folge 3 GmbH und Gärtner Datensystem GmbH & Co. KG durchgeführt. Die entsprechende Weitergabe ist zur Vertragserfüllung erforderlich (Art. 6 Abs. 1 lit. b) DSGVO).

Wir speichern Ihre personenbezogenen Daten zu den genannten Zwecken für die Dauer des Bestehen Ihres SSO-Accounts.

Für Supportanfragen stellen wir ein Postfach unter der E-Mailadresse ranking@zeit.de zur Verfügung. Dieses Postfach wird sowohl von ZEIT Online als auch von Centrum für Hochschulentwicklung GmbH (Verler Straße 6, 33332 Gütersloh, Telefon 05241 97 61 0, Telefax 05241 9761 40, E-Mail info@che.de, Internet: www.che.de) verwaltet, um Anfragen rund um das Thema Hochschulranking sachkundig beantworten zu können.  Zur Beantwortung Ihre Anfrage werden Ihre E-Mailadresse sowie alle weiteren in Ihrer Anfrage freiwillig angegebenen personenbezogenen Daten verarbeitet. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b) DSGVO. Die im Rahmen Ihrer Anfrage übermittelten personenbezogenen Daten werden von uns zur Bearbeitung der Anfrage und für den Fall von Anschlussfragen in der Regel für die Dauer von sechs Monaten gespeichert. Haben wir Ihre personenbezogenen Daten bereits im Zuge Ihrer Registrierung für einen unserer Dienste (z.B. SSO-Account) erhalten, werden diese Daten weiterhin für die Dauer des Bestehens Ihrer Registrierung gespeichert.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#g-che-hochschulranking)

**h.) ZEIT-Stellenmarkt**

Auf unserer [Internetseite](https://jobs.zeit.de/) haben Sie die Möglichkeit ohne Angabe von persönlichen Daten den ZEIT-Stellenmarkt zu durchsuchen. Möchten Sie, dass Ihr Suchprofil gespeichert wird, ist es notwendig, dass Sie zunächst ein (ZEIT-Stellenmarkt-Konto) anlegen und sich unter Angabe Ihrer E-Mailadresse registrieren.

Die Erhebung der E-Mailadresse und des Suchprofils dient dazu, Ihnen, sofern Sie sich als Job suchend melden, aktuelle auf Ihr Profil passende Stellenangebote sowie weitere interessante Informationen des Jobmarkts im Rahmen des Newsletters zuzustellen. Eine Abmeldung vom Newsletter ist jederzeit möglich, indem Sie Ihre Registrierung gänzlich löschen. Eine entsprechende Löschung können Sie entweder in Ihren Profileinstellungen oder durch einen Klick auf den entsprechenden Link, welcher in jedem Newsletter enthalten ist, vornehmen.

Ohne die Erstellung eines Suchprofils können wir Ihnen die aktuellen Stellenangebote im Rahmen des Newsletters nicht zusenden. Die Angabe dieser Daten ist somit zur entsprechenden Vertragserfüllung notwendig und beruht insoweit auf Art. 6 Abs. 1 lit. b) DSGVO. Die Angabe von Anrede, Titel, Name und Vorname ist freiwillig. Sofern Sie uns diese Daten nicht mitteilen, erleiden Sie hierdurch keinerlei Nachteile. Die Verarbeitung der von Ihnen freiwillig angegebenen Daten beruht auf Art. 6 Abs. 1 lit. a) DSGVO.

Ihre Daten werden, sofern eine entsprechende Einwilligung Ihrerseits vorliegt, zudem an unsere Kooperationspartner, die ZEIT-Verlagsgruppe zum Zwecke der Werbung weitergegeben. Diese Weitergabe beruht auf unserem entsprechenden unternehmerischen Interesse und damit auf Art. 6 Abs. 1 lit. f) DSGVO.

Ihre Daten werden gelöscht, sobald für die Erreichung des Zwecks ihrer Erhebung nicht mehr erforderlich sind. Ihre E-Mailadresse wird demnach solange gespeichert, wie Ihre Registrierung fortbesteht und das Abonnement des Newsletters aktiv ist. Bei weiteren Fragen oder Anliegen zu Ihren Daten auf dem ZEIT Stellenmarkt wenden Sie sich bitte an [jobs@zeit.de](mailto:jobs@zeit.de?subject=Datenschutzanfrage)

Die Datenverarbeitung findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#h-zeit-stellenmarkt)

**i.) Kontaktaufnahme**

Nehmen Sie per Formular auf unserer Internetseite oder per E-Mail Kontakt zu uns auf, erhalten wir ebenfalls personenbezogene Daten von Ihnen. Diese Daten werden von uns zur Bearbeitung der Anfrage (vgl. Art. 6 Abs. 1 lit b DSGVO) und für den Fall von Anschlussfragen für die Dauer von sechs Monaten gespeichert.

Diese Daten verwenden wir weder zu Werbezwecken, noch geben wir Sie ohne eine diesbezügliche Einwilligung Ihrerseits weiter, es sei denn, dass dies zur Erfüllung des Vertrages erforderlich ist.

Die Datenverarbeitung im Rahmen unserer Kundenbetreuung findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie  in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit) .

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#i-kontaktaufnahme)

**j.) Kommentierung von Beiträgen / Forennutzung und Blog**

Auf unserer Webseite bieten wir [Blogs](https://www.zeit.de/blogs/index) und die ZEIT [Community](https://www.zeit.de/community/index) an. In diesem Blog veröffentlichen wir Beiträge zu verschiedenen Themen. Zu den jeweiligen Beiträgen können Sie Kommentare abgeben. Wenn Sie einen Kommentar abgeben, wird dieser mit dem von Ihnen angegebenen Nutzernamen dem jeweiligen Beitrag zugeordnet veröffentlicht. Wir empfehlen Ihnen bei der Wahl des Nutzernamens insoweit anstatt Ihres Klarnamens die Verwendung eines Pseudonyms. Zur Nutzung der Kommentarfunktion ist die Angabe des von Ihnen gewählten Nutzernamens sowie Ihrer E-Mailadresse Pflicht. Alle weiteren von Ihnen gemachten Angaben sind freiwillig. Wenn Sie einen Kommentar abgeben, speichern wir zu den vorgenannten Daten Ihre IP-Adresse.

Die Speicherung Ihrer E-Mailadresse erfolgt zu dem Zweck, um mit Ihnen Kontakt aufzunehmen, falls ein Dritter Ihren Kommentar als rechtswidrig bei uns meldet. Ihre IP-Adresse speichern wir zu dem Zweck, um uns im Falle der Veröffentlichung rechtswidriger Inhalte durch Sie gegen Ansprüche Dritter verteidigen zu können.

Wir behalten uns vor, Kommentare zu löschen, wenn Sie von Dritten als rechtswidrig beanstandet werden.

Ihre E-Mailadresse speichern wir, solange Ihr Kommentar öffentlich sichtbar ist. Ihre IP-Adresse löschen wir eine Woche, nachdem Sie den Kommentar veröffentlicht haben.

Wir verarbeiten Ihre Daten auf Grundlage der von Ihnen erteilten Einwilligung und damit gemäß Art. Art. 6 Abs. 1 lit. a) DSGVO. Sie können Ihre Einwilligung jederzeit widerrufen und der Speicherung der vorstehenden Daten jederzeit widersprechen.

Die Datenverarbeitung findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

Zusätzlich bieten wir einen Service an, bei dem Sie per E-Mail informiert werden, wenn weitere Nutzer einen Kommentar zu Ihrem Beitrag hinterlassen. Um diesen Service nutzen zu können, müssen Sie beim Schreiben Ihres Kommentars die Checkbox "E-Mail-Service" aktivieren. Für diesen Service verwenden wir das sog. Double-Opt-In Verfahren. Wenn Sie unter Aktivierung der Checkbox einen Kommentar veröffentlichen, erhalten Sie eine E-Mail, in der Sie Ihre E-Mailadresse und den Wunsch des künftigen Erhalts unserer Benachrichtigungs-E-Mails bestätigen müssen.

Ihre personenbezogenen Daten für den oben beschriebenen "E-Mail-Service", inklusive E-Mailadresse, Ihre Zeitpunkte der Registrierung für den Service und Ihre IP-Adresse werden von uns gespeichert, bis Sie sich von dem Hinweis-Service abmelden. Die Benachrichtigungen können Sie jederzeit abbestellen, indem Sie auf den in der E-Mail enthaltenen Link klicken.

Die rawr-Kommentierungsfunktion ist ein Produkt der rawr GmbH. Rawr ist ein interaktives Kommentarsystem, das es Ihnen als Leser ermöglicht, auf unserer Website unter Zustimmung oder Ablehnung zu einer Frage Kommentare zu hinterlassen. Nähere Informationen zu rawr und seinen Funktionen finden Sie unter [rawr.at](https://www.rawr.at/). Nach Registrierung als ZEIT-User können Sie die Kommentar-Funktion von rawr nutzen. Der für unsere Online-Angebote unter [meine.zeit.de](https://meine.zeit.de/anmelden) registrierte und angemeldete User gibt seine Kommentare in eine auf unserer Website eingebettete Maske von rawr ein und akzeptiert die Nutzungsbedingungen von rawr.

Hinsichtlich der Erhebung, Verarbeitung und Nutzung der betreffenden Daten gelten die Nutzungsbedingungen und Datenschutzhinweise von rawr, die Sie unter [rawr.at/agbs](https://www.rawr.at/agbs) finden. Wenn ein Nutzer die Kommentarfunktion des Dienstes nutzt, übermitteln wir E-Mailadresse und ein Identifikationsmerkmal an rawr. Die E-Mailadresse wird benötigt, um den Absender eines Kommentars zu benennen und wird nur zu diesem Zweck an rawr weitergegeben. Damit die Kommentare auf unserer Webseite veröffentlicht werden können, übermittelt rawr an unser Onlineangebot den Kommentartext samt des Identifikationsmerkmals. Die Administratoren und Moderatoren, die bei uns für die Kommentare zuständig sind, erhalten Zugriff auf diese Daten.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#j-kommentierung-von-beitraegen-forennutzung-und-blog)

**k.) ZEIT Akademie**

Schließen Sie auf unserer [Internetseite](https://www.zeitakademie.de/) ein Abonnement der ZEIT Akademie ab, so ist hierfür die Angabe der folgenden Daten notwendig: Vorname, Name, Adresse, E-Mail. Ihre Telefonnummer können Sie freiwillig eintragen, Ihre Bankdaten benötigen wir dann, wenn Sie eine Zahlung im Lastschriftverfahren wünschen. Die genannten Daten benötigen wir, um den geschlossenen Abonnementvertrag zu erfüllen. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b) DSGVO. Rechtsgrundlage für die Verarbeitung der freiwillig eingetragenen Daten ist Art. 6 Abs. 1a) DSGVO.

Wir geben Ihre Daten zum Zwecke der Abwicklung des Abonnements weiter an die DPV Deutscher Pressevertrieb GmbH, Am Baumwall 11, 20459 Hamburg. Wenn Sie an Umfragen teilnehmen, die auf unserer Seite angeboten werden, werden Daten an TYPEFORM S.L., Carrer Bac de Roda, 163, 08018 Barcelona, Spanien übertragen.

Zur Bereitstellung der Website werden Dienste über der Firma Savvii B.V., Oranjesingel 76, 6511 NZ Nijmegen – Niederlande genutzt. Darüber hinaus nutzen wir Dienste der DigitalOcean, LLC, 101 6th Ave, New York, USA. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Die Datenweitergabe ist zur Vertragserfüllung erforderlich und beruht auf Art. 6 Abs. 1 lit. b) DSGVO. Ihre persönlichen Daten werden für die Dauer des bestehenden Vertrages gespeichert. Darüber hinaus speichern wir gemäß Art. 6 Abs. 1 lit c) DSGVO personenbezogene Daten zur Erfüllung unserer gesetzlichen Aufbewahrungspflichten nach § 257 Abs. 4 HGB, § 147 Abs. 3 AO. Dies betrifft z.B. Eintragungen im Kontokorrentbuch, Buchungsbelege und Rechnungen zu Ihrem Abonnement. Die Aufbewahrungsfrist beträgt maximal zehn Jahre und beginnt mit dem Schluss des Kalenderjahres, in dem die letzte Eintragung in das Buch gemacht oder der Buchungsbeleg entstanden ist, ferner die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind Im Anschluss werden Ihre Daten gelöscht.

Die Datenverarbeitung findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#k-zeit-akademie)

**l.) ZEIT Reisen**

Buchen Sie eine Reise in unserem Reiseportal <https://zeitreisen.zeit.de/> ist zur Vertragserfüllung die Angabe der folgenden Daten notwendig: Vorname, Name, Adresse, Geburtsdatum. Ihre Telefonnummer können Sie freiwillig eintragen, Ihre Bankdaten benötigen wir dann, wenn Sie eine Zahlung im Lastschriftverfahren wünschen. Rechtsgrundlage für die Datenverarbeitung ist hinsichtlich der Pflichtdaten Art. 6 Abs. 1 lit. b) DSGVO, hinsichtlich weitere Daten Art. 6 Abs. 1 lit. a) DSGVO.

Es findet eine Weitergabe Ihrer Daten an Kohlenberg Software für die Abwicklung der ZEIT Reise Buchung sowie an die die Reise durchführenden Unternehmen (Hotels, Airlines, Schiffe etc.) statt. Die Weitergabe ist zur Vertragserfüllung notwendig, Art. 6 Abs. 1 lit. b) DSGVO.

Bestellen Sie einen Katalog in unserem Reiseportal <https://zeitreisen.zeit.de/>, sind zur Abwicklung Ihrer Bestellung die Angabe der folgenden Daten notwendig: Vorname, Name, Adresse. Ihre E-Mailadresse und Telefonnummer können Sie freiwillig eintragen. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b) bzw. a) DSGVO.

Zur Abwicklung der Katalogbestellung werden Ihre Daten an einen Dienstleister, welcher den Versand für uns übernimmt weitergegeben. Die Weitergabe ist zur Vertragserfüllung notwendig, Art. 6 Abs. 1 lit. b) DSGVO.

Das Hosting und die Weiterentwicklung der Website ZEIT Reisen findet statt durch FUERSTVONMARTIN GmbH und beruht auf einem entsprechenden Interesse unseres Unternehmens (Art. 6 Abs. 1 f) DSGVO).

Ihre persönlichen Daten werden zu den genannten Zwecken bis zur Erfüllung des bestehenden Vertrages gespeichert. Darüber hinaus speichern wir gemäß Art. 6 Abs. 1 lit c) DSGVO personenbezogene Daten zur Erfüllung unserer gesetzlichen Aufbewahrungspflichten nach § 257 Abs. 4 HGB, § 147 Abs. 3 AO. Dies betrifft z.B. Eintragungen im Kontokorrentbuch, Buchungsbelege und Rechnungen zu Ihrer Buchung. Die Aufbewahrungsfrist beträgt maximal zehn Jahre und beginnt mit dem Schluss des Kalenderjahres, in dem die letzte Eintragung in das Buch gemacht oder der Buchungsbeleg entstanden ist, ferner die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind. Im Anschluss werden Ihre Daten gelöscht.

Die Datenverarbeitung findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#l-zeit-reisen)

**m.) Freunde der ZEIT**

Auf unserer [Internetseite](http://verlag.zeit.de/freunde/) bieten wir Ihnen die Möglichkeit, sich für unser Programm "Freunde der ZEIT" zu registrieren. Hierfür ist es notwendig, dass Sie zunächst einen SSO-Account anlegen und sich unter Angabe Ihrer E-Mailadresse registrieren. Weitere Infos zur Verarbeitung der Daten in dem Zusammenhang mit der Erstellung des SSO-Accounts finden Sie unter der entsprechenden Überschrift ["SSO-Account"](https://www.zeit.de/hilfe/datenschutz#d-sso-account).

Danach können Sie Ihre Registrierung für "Freunde der ZEIT" abschließen. Es ist die Angabe der folgende Daten notwendig.

− Name  
− postalische Adresse  
− E-Mailadresse  
− Geburtsdatum (freiwillige Angabe)

Ihre Daten wird für die Dauer Ihrer Registrierung gespeichert. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b) bzw. hinsichtlich der freiwillig gemachten Angabe Art. 6 abs. 1 a) DSGVO.

Mit der Registrierung für Freunde der ZEIT ist es Ihnen möglich, Veranstaltungen im Rahmen des Programms zu besuchen. Hierfür geben wir die Daten an die doo GmbH, St.-Martin-Straße 58-68, 81541 München für die Buchung der Veranstaltungen weiter. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b) DSGVO.

Die Webseite [www.freundederzeit.de](http://www.freundederzeit.de/) wird von TEMPUS CORPORATE GmbH, Buceriusstraße, Eingang Speersort 1, 20095 Hamburg betreut. Eine Datenweitergabe beruht auf unserem berechtigten Interesse und damit auf Art. 6 Abs. 1f) DSGVO. Die Datenverarbeitung findet in gemeinsamer Verantwortlichkeit statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

Wenn Sie an einer Umfrage auf unserer Seite teilnehmen werden Ihre Daten an die Firma JotForm Inc., 111 Pine St. Suite 1815, San Francisco, CA 94111, USA weitergegeben. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#m-freunde-der-zeit)

**n.) Nutzung Ihrer Daten zu Werbezwecken**

Erhalten wir Ihre Daten im Zusammenhang mit einem Vertragsabschluss oder einer Registrierung für unsere Dienste, behalten wir es uns vor, diese auch zu Werbezwecken zu verarbeiten. Wir verarbeiten Ihre unter den im Folgenden genannten Bedingungen zu Werbezwecken für eigene ähnliche Angebote und Angebote von Partnerunternehmen und geben Ihre Daten außerdem zum Zweck der Werbung durch Dritte weiter.

(1) Werbung für eigene ähnliche Angebote

Die von Ihnen bei uns gespeicherten persönlichen Daten verwenden wir zur Werbung für eigene ähnliche Angebote der [ZEIT-Verlagsgruppe](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit)[.](https://www.zeit.de/hilfe/datenschutz" \l "_msocom_17" \t "_blank)

Erhalten wir Ihre E-Mailadresse im Zusammenhang mit einem Vertragsabschluss im weiteren Sinne (Abonnement, Bestellung im Shop, Registrierung für einen Newsletter, für Z+, SIT, BOA oder einen ähnlichen Dienst), ist es uns gestattet, Ihnen an Ihre E-Mailadresse Angebote für Waren und Dienstleistungen aus unserem Haus zuzusenden, die den von Ihnen in Anspruch genommenen Dienstleistungen ähnlich sind. An der entsprechenden Zusendung von Werbeangeboten haben wir ein unternehmerisches Interesse. Die Verarbeitung Ihrer E-Mailadresse beruht insoweit auf einem berechtigten Interesse. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f) DSGVO i.V.m. § 7 Abs. 3 UWG.

**Einer Verarbeitung Ihrer Daten zum Zwecke der Direktwerbung können Sie jederzeit widersprechen.**

Haben Sie uns eine Einwilligung in die Zusendung von Werbeemails erteilt, beruht die entsprechende Verarbeitung zudem auf Art. 6 Abs. 1 lit a) DSGVO. Eine erteilte Einwilligung können Sie jederzeit, beispielsweise per E-Mail an [email@zeit.de](mailto:email@zeit.de) widerrufen.

Wir speichern Ihre Daten zu Werbezwecken solange uns kein entsprechender Widerruf / Widerspruch vorliegt.

(2) Weitergabe Ihrer Daten zum Zwecke der Werbung durch Dritte

Neben der Werbung für eigene Produkte vergeben wir die bei uns gespeicherten postalischen Kontaktdaten auch an einen Marketingdienstleister, welcher Ihre Daten nutzt, um Ihnen interessante Werbeangebote von Dritten zuzusenden. Sollte Ihre Adresse von dem Marketingdienstleister zum Zwecke der Werbung für Drittangebote verwendet werden, werden Sie in dem Postmailing darauf hingewiesen, dass Ihre Adresse von uns an den Marketingdienstleister weitergegeben wurde.

An der Weitergabe von persönlichen Daten an den Marketingdienstleister zum Zwecke der Werbung durch Dritte haben wir ein unternehmerisches Interesse. Die Datenverarbeitung beruht insoweit auf Art. 6 Abs. 1 lit. f) DSGVO.

Sie können sich gerne jederzeit an uns wenden und erfragen, ob wir Ihre Adresse zu Werbezwecken weitergegeben haben. Haben Sie in den Erhalt der Werbung von Dritten eingewilligt, beruht die entsprechende Verarbeitung zudem auf Art. 6 Abs. 1 lit a) DSGVO Der Weitergabe und der **Verarbeitung Ihrer Daten zum Zwecke der Direktwerbung können Sie jederzeit widersprechen,**beispielsweise per E-Mail an [email@zeit.de](mailto:email@zeit.de)

Solange uns jedoch kein entsprechender Widerspruch vorliegt und unser Interesse an einer entsprechenden Verarbeitung Ihrer Daten fortbesteht, speichern wir Ihre Daten zu Werbezwecken.

(3) Speicherung der Daten in unserem Data Warehouse

Zur Analyse und Kontrolle unserer Werbemaßnahmen speichern wir Ihre Daten in einer separaten Datenbank, Data Warehouse genannt. Hier werden Ihre personenbezogenen Daten gespeichert und strikt von den Auftragsdaten getrennt. Letztere stehen für Analyse- und Reportingzwecke pseudonymisiert zur Verfügung. Auf Basis der Auftragsdaten nutzen wir die Informationen zur Kontrolle und Optimierung der Werbemaßnahmen. Nur für spezielle Fragestellungen werden die Daten zur Gruppen-Profilbildung sowie zur Erstellung von Engagement und Propensity Score genutzt.

Die getrennten personenbezogenen Daten unterliegen bei uns einem besonderen Schutz und werden nur für die Selektion für Werbezwecke genutzt.

Die Datenverarbeitung im Data Warehouse findet in gemeinsamer Verantwortlichkeit mit anderen Unternehmen der ZEIT Verlagsgruppe statt. Näheres dazu finden Sie in [Abschnitt V](https://www.zeit.de/hilfe/datenschutz#teil-v-gemeinsame-verantwortlichkeit).

Die Verarbeitung Ihrer Daten beruht insoweit auf einem berechtigten Interesse und damit auf Art. 6 Abs. 1 lit. f) DSGVO. Der Verarbeitung können Sie jederzeit, beispielsweise per E-Mail an [email@zeit.de](mailto:email@zeit.de) widersprechen.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#n-nutzung-ihrer-daten-zu-werbezwecken)

**o.) ZEIT Campus Berufsorientierungsangebot (BOA)**

Das Berufsorientierungsangebot erfolgt durch den Anbieter ZEIT ONLINE GmbH, Speersort 1, 20095 Hamburg in Kooperation mit der talentsconnect AG (ehemalig 22CONNECT AG), Domstraße 55-73, 50668 Köln

Nachstehende Regelungen informieren Sie insoweit über die Art, den Umfang und den Zweck der Erhebung, die Nutzung und die Verarbeitung von personenbezogenen Daten durch talentsconnect AG in Kooperation mit ZEIT ONLINE GmbH als verantwortliche Stelle im Sinne des Datenschutzrechts. Die Datenschutzerklärung von talentsconnect AG finden sie [hier](https://www.talentsconnect.com/privacy).

**Gegenstand des Datenschutzes**

ZEIT Online GmbH in Zusammenarbeit mit [talentsconnect AG](https://www.talentsconnect.com/)  
optimieren flexibel den gesamten Recruitingprozess. Gegenstand des Datenschutzes sind personenbezogene Daten. Diese sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hierunter fallen z.B. Angaben wie Name, Post-Adresse, E-Mailadresse oder Telefonnummer, ggf. aber auch Nutzungsdaten. Nutzungsdaten sind solche Daten, die erforderlich sind, um unsere Webseiten zu nutzen, wie zum Beispiel Angaben über Beginn, Ende und Umfang der Nutzung unserer Webseite und Anmeldedaten. Welche Daten von uns erhoben werden und wie diese verarbeitet oder genutzt werden, wird im Folgenden beschrieben:

Die Eingabe der Daten bei BOA erfolgt freiwillig und ohne Pflicht. Die Entscheidung welche Daten im Rahmen der Nutzung bereitgestellt werden sollen entscheidet der BOA-Nutzer selbst. Aus technischen und funktionellen Gründen ist in manchen Fällen die Angabe von Daten erforderlich, um BOA nutzen zu können. In den folgenden Absätzen wird beschrieben, welche Daten verpflichtend eingegeben werden müssten.

**1. Von BOA-Nutzern angegebene Daten**

**Datenverarbeitungen zur Vertragsdurchführung**

Nach Registrierung eines Nutzers in [SSO](https://www.zeit.de/hilfe/datenschutz#d-sso-account) durchläuft der BOA-Nutzer den BOA-Persönlichkeitstest. Dieser kann verschiedene BOA-Funktion verwenden, die auf die freiwillig angegebenen personenbezogenen Daten zurückgreifen. So werden unter Angabe der personenbezogenen Daten (Anrede, Name und E-Mailadresse) zukünftige Jobangebote per E-Mail als BOA-Mailing zu gesendet.

Zum Zwecke der Nutzung und Vertragsausführung des Berufsorientierungsangebotes finden Datenübertragungen von ZEIT Online GmbH an 22connect AG und umgekehrt auf der Grundlage von Art. 6 Abs. 1 Buchst. b DSGVO statt.

Im Übrigen erfolgt grundsätzlich keine Weitergabe der personenbezogenen Daten ohne Ihre ausdrückliche Einwilligung, soweit keine gesetzliche oder gerichtliche Verpflichtung zur Weitergabe, insbesondere an Strafverfolgungsbehörden, Finanzbehörden oder sonstige öffentliche Stellen besteht.

**Datenverarbeitung mit Einwilligung**

Die Weitergabe personenbezogener Daten (Angaben aus dem Berufsprofil wie Name, E-Mailadresse, Telefonnummer, die drei stärksten Persönlichkeitsdimensionen sowie freigegebene Dokumente) erfolgt nur mit ausdrücklicher Zustimmung, für jede einzelne Übermittlung. Es gibt zwei Möglichkeiten dieser Übermittlung:

●      Bei Bewerbung auf ein Jobangebot können mit einem Klick auf den "Bewerben"-Button personenbezogene Daten für dieses Unternehmen freigeben werden.

●      Wenn ein Unternehmen Interesse zeigt, sendet BOA Ihnen eine Freigabeanfrage per E-Mail, über die Ihre Zustimmung der Weitergabe Ihrer personenbezogener Daten an dieses Unternehmen freigeben werden können.

Die Einwilligung von Kindern unter 16 Jahren ist nur dann wirksam, wenn sie von den Eltern stammt oder mit deren Zustimmung erfolgt. Ein Widerruf der Einwilligung ist selbstverständlich jederzeit möglich.

Wir verarbeiten die vorab genannten personenbezogenen Daten im Einklang mit den Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) (neue Fassung) sowie weiteren einschlägigen Fachgesetzen:

Die Datenverarbeitung erfolgt auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Sie können diese Einwilligung jederzeit widerrufen. Die Rechtmäßigkeit der bereits erfolgten Datenverarbeitungsvorgänge bleibt vom Widerruf unberührt.

BOA benötigt die Beantwortung der Fragen aus dem Berufspersönlichkeitstest, um ein Testergebnis mit BOA-Nutzer-Profil anzulegen und mittels eines Matching-Verfahrens passende Berufsbilder und passende Stellenanzeigen gelistet anbieten zu können. Dies ermöglicht dem BOA-Nutzer eine Vorsortierung aller Ergebnisse, die im Wesentlichen aufgrund von Filtern gesteuert sind und daher nicht als Profiling zu verstehen sind.

BOA bietet als freiwillige Möglichkeit das BOA-Nutzer-Profil zu ergänzen und zu personalisieren. Dafür können beispielsweise Angaben zur: Adresse, Geschlecht, Geburtsdatum, Interessen, Fähigkeiten sowie Abschlüssen und Berufslaufbahn eingestellt werden. Weiter kann ein Foto auf der Profilseite hochgeladen werden. Diese Angaben sind freiwillig und nicht notwendig, um sich anzumelden und BOA zu nutzen.

**Widerruf Ihrer Einwilligung zur Datenverarbeitung bei BOA**

Viele Datenverarbeitungsvorgänge sind nur mit Ihrer ausdrücklichen Einwilligung möglich. Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Dazu reicht eine formlose Mitteilung per E-Mail an [boa@zeit.de](mailto:boa@zeit.de). Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

**Weitergabe von Daten**

Grundsätzlich erfolgt die Weitergabe Ihrer personenbezogenen Daten ohne Ihre ausdrückliche vorherige Einwilligung nur in den nachfolgend genannten Fällen:

●      Wenn es zur Aufklärung einer rechtswidrigen Plattform Nutzung dient oder für die Rechtsverfolgung erforderlich ist, werden personenbezogene Daten an die Strafverfolgungsbehörden sowie gegebenenfalls an geschädigte Dritte weitergeleitet. Dies geschieht jedoch nur dann, wenn konkrete Anhaltspunkte für ein gesetzwidriges beziehungsweise missbräuchliches Verhalten vorliegen. Eine Weitergabe kann auch dann stattfinden, wenn dies der Durchsetzung von Nutzungsbedingungen oder anderer Vereinbarungen dient. ZEIT Online GmbH ist zudem gesetzlich verpflichtet, auf Anfrage bestimmten öffentlichen Stellen Auskunft zu erteilen. Dies sind Strafverfolgungsbehörden, Behörden, die bußgeldbewährte Ordnungswidrigkeiten verfolgen und die Finanzbehörden.

●      Gelegentlich sind wir für die Erbringung der Dienstleistungen auf vertraglich verbundene Fremdunternehmen und externe Dienstleister angewiesen, beispielsweise in den Bereichen der Übersendung von Werbemaßnahmen (nur, sofern Sie diesen vorher explizit zugestimmt haben) sowie dem Kundenservice. In solchen Fällen werden Informationen an diese Unternehmen bzw. Einzelpersonen weitergegeben, um diesen die weitere Bearbeitung zu ermöglichen. Diese externen Serviceprovider werden von uns sorgfältig ausgewählt und regelmäßig überprüft, um sicherzugehen, dass Ihre Privatsphäre gewahrt bleibt. Die Serviceprovider dürfen die Daten ausschließlich zu den von ZEIT Online und talentsconnect AG vorgegebenen Zwecken verwenden. Die Serviceprovider werden darüber hinaus von ZEIT Online und oder talentsconnect AG vertraglich verpflichtet, Ihre Daten ausschließlich gemäß dieser Datenschutzerklärung sowie im Rahmen der DSGVO zu behandeln.

**Löschung Ihrer Daten**

Soweit Ihre Daten für die vorgenannten Zwecke nicht mehr erforderlich sind, werden sie gelöscht. Wenn Sie eine Löschung Ihrer Daten wünschen, senden Sie bitte eine E-Mail an [email@zeit.de](mailto:email@zeit.de). In diesem Fall werden die personenbezogenen Daten vollständig und endgültig gelöscht. Soweit Daten aus gesetzlichen Gründen aufbewahrt werden müssen, werden diese bis zur endgültigen Löschung eingeschränkt in der Verarbeitung und somit gesperrt. Die Daten stehen einer weiteren Verwendung dann nicht mehr zur Verfügung.

**Weitere Informationen über Ihre Rechte finden Sie im**[**Abschnitt IV**](https://www.zeit.de/hilfe/datenschutz#teil-iv-ihre-rechte)

**Cookies**

ZEIT Online GmbH und talentsconnect AG speichern sogenannte "Cookies", um Ihnen einen umfangreichen Funktionsumfang zu bieten und die Nutzung unserer Webseiten komfortabler zu gestalten, insbesondere für Authentifizierungszwecke. "Cookies" sind kleine Dateien, die mit Hilfe Ihres Internetbrowsers auf Ihrem Rechner gespeichert werden. Cookies richten auf Ihrem Rechner keinen Schaden an und enthalten keine Viren. Die meisten, der von uns verwendeten Cookies, sind so genannte "Session-Cookies". Sie werden nach Ende Ihres Besuchs automatisch gelöscht. Andere Cookies bleiben auf Ihrem Endgerät gespeichert, bis Sie diese löschen. Diese Cookies ermöglichen es uns, Ihren Browser beim nächsten Besuch wiederzuerkennen. Wenn Sie den Einsatz von "Cookies" nicht wünschen, können Sie das Speichern von "Cookies" auf Ihrem Rechner durch entsprechende Einstellungen Ihres Internetbrowsers verhindern. Bitte beachten Sie, dass die Funktionsfähigkeit und der Funktionsumfang unseres Angebots dadurch eingeschränkt sein können.

**BOA-Newsletter**

Mit den nachfolgenden Hinweisen klären wir Sie über die Inhalte unseres BOA-Newsletters, BOA-E-Mailings, sowie das Anmelde-, Versand- und das statistische Auswertungsverfahren sowie Ihre Widerspruchsrechte auf. Indem Sie unseren BOA-Newsletter oder BOA-E-Mailing abonnieren, erklären Sie sich mit dem Empfang und den beschriebenen Verfahren einverstanden.

ZEIT Online GmbH behält sich vor Ihnen einen kostenlosen BOA-Newsletter Service anzubieten. Mit dem BOA-Newsletter informiert ZEIT Online GmbH über neue Funktionalitäten, neue Werbekampagnen, die Teilnahme an Umfragen, um Sie auf neue Produkte oder Dienstleistungen aufmerksam zu machen oder Ihnen andere Informationen zukommen zu lassen, die für Sie möglicherweise von Interesse sind. Weiterhin informieren wir Sie gegebenenfalls im BOA-Newsletter über Angebote und Produkte unserer Kooperationspartner.

Die Anmeldung zu unserem BOA-Newsletter erfolgt in einem sog. Double-Opt-In-Verfahren. D.h. Sie erhalten nach der Anmeldung über den [SSO-Account](https://www.zeit.de/hilfe/datenschutz#d-sso-account) eine E-Mail, in der Sie um die Bestätigung Ihrer Anmeldung gebeten werden. Diese Bestätigung ist notwendig, damit sich niemand mit fremden E-Mailadressen anmelden kann. Weitere Informationen zu unseren Newsletterpartnern finden Sie im Abschnitt  [Newsletterregistrierung](https://www.zeit.de/hilfe/datenschutz#c-registrierung-newsletter) .

**BOA-E-Mailing**

ZEIT Online GmbH und talentsconnect AG bieten Ihnen auf der BOA-Seite die Möglichkeit, das BOA-E-Mailing zu bestellen, welches Sie über Stellenangebote informiert. Um unsere BOA-E-Mailings empfangen zu können, nutzen wir Ihre im SSO-Account angegebene E-Mailadresse. Das Abonnement dieses Newsletters können Sie jederzeit kündigen.

Der Versand der BOA-E-Mailings erfolgt mittels "MailChimp", einer Newsletterversand Plattform des US-Anbieters Rocket Science Group, LLC, 675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, USA.

Die E-Mailadressen unserer BOA-E-Mailings, als auch deren weitere, im Rahmen dieser Hinweise beschriebenen Daten, werden auf den Servern von MailChimp in den USA gespeichert. MailChimp verwendet diese Informationen zum Versand und zur Auswertung der Newsletter in unserem Auftrag. Des Weiteren kann MailChimp nach eigenen Informationen diese Daten zur Optimierung oder Verbesserung der eigenen Services nutzen, z.B. zur technischen Optimierung des Versandes und der Darstellung der BOA-E-Mailings oder für wirtschaftliche Zwecke, um zu bestimmen aus welchen Ländern die Empfänger kommen. MailChimp nutzt die Daten unserer BOA-E-Mailing-Empfänger jedoch nicht, um diese selbst anzuschreiben oder an Dritte weiterzugeben.

Wir vertrauen auf die Zuverlässigkeit und die IT- sowie Datensicherheit von MailChimp. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender). Des Weiteren hat 22connect  mit MailChimp ein "Data-Processing-Agreement" abgeschlossen. Dabei handelt es sich um einen Vertrag, in dem sich MailChimp dazu verpflichtet, die Daten unserer Nutzer zu schützen, entsprechend deren Datenschutzbestimmungen in unserem Auftrag zu verarbeiten und insbesondere nicht an Dritte weiter zu geben.

**Statistische Erhebung und Analysen**  
Die BOA-E-Mailings enthalten einen sog. "web-beacon", d.h. eine pixelgroße Datei, die beim Öffnen des BOA-E-Mailings von dem Server von MailChimp abgerufen wird. Im Rahmen dieses Abrufs werden zunächst technische Informationen, wie Informationen zum Browser und Ihrem System, als auch Ihre IP-Adresse und Zeitpunkt des Abrufs erhoben. Diese Informationen werden zur technischen Verbesserung der Services anhand der technischen Daten oder der Zielgruppen und ihres Leseverhaltens anhand derer Abruforte (die mit Hilfe der IP-Adresse bestimmbar sind) oder der Zugriffszeiten genutzt.

Zu den statistischen Erhebungen gehört ebenfalls die Feststellung, ob die BOA-E-Mailings geöffnet werden, wann sie geöffnet werden und welche Links geklickt werden. Diese Informationen können aus technischen Gründen zwar den einzelnen BOA-E-Mailing-Empfängern zugeordnet werden. Es ist jedoch weder unser Bestreben, noch das von MailChimp, einzelne Nutzer zu beobachten. Die Auswertungen dienen uns viel mehr dazu, die Lesegewohnheiten unserer Nutzer zu erkennen und unsere Inhalte auf sie anzupassen oder unterschiedliche Inhalte entsprechend den Interessen unserer Nutzer zu versenden.

**Online-Aufruf und Datenmanagement**  
Es gibt Fälle, in denen wir die BOA-E-Mailing-Empfängern auf die Webseiten von MailChimp leiten, z.B. enthalten unsere BOA-E-Mailings einen Link, mit dem die BOA-E-Mailing-Empfänger die BOA-E-Mailings online abrufen können (z.B. bei Darstellungsproblemen im E-Mailprogramm). Ferner können BOA-E-Mailing-Empfänger ihre Daten, wie z.B. die E-Mailadresse nachträglich korrigieren. Ebenso ist die Datenschutzerklärung von MailChimp nur auf deren Seite abrufbar.

In diesem Zusammenhang weisen wir darauf hin, dass auf den Webseiten von MailChimp Cookies eingesetzt und damit personenbezogene Daten durch MailChimp, deren Partnern und eingesetzten Dienstleistern verarbeitet werden. Auf diese Datenerhebung haben wir keinen Einfluss. Weitere Informationen können Sie der Datenschutzerklärung von MailChimp entnehmen.

**Kündigung/Widerruf**Sie können das BOA-E-Mailing jederzeit abbestellen. Jedes BOA-E-Mailing enthält die Information, wie die BOA-E-Mailings durch Sie mit Wirkung für die Zukunft abbestellt werden kann.

Damit erlöschen gleichzeitig Ihre Einwilligungen in dessen Versand via MailChimp und die statistischen Analysen. Ein getrennter Widerruf des Versandes via MailChimp oder der statistischen Auswertung ist leider nicht möglich.

**Rechtsgrundlagen Datenschutz-Grundverordnung**  
Entsprechend den Vorgaben der ab dem 25. Mai 2018 geltenden Datenschutz-Grundverordnung (DSGVO) informieren wir Sie, dass die Einwilligungen in den Versand der E-Mailadressen auf Grundlage der Art. 6 Abs. 1 lit. a, 7 DSGVO sowie § 7 Abs. 2 Nr. 3, bzw. Abs. 3 UWG erfolgt. Der Einsatz des Versanddienstleisters MailChimp, Durchführung der statistischen Erhebungen und Analysen sowie Protokollierung des Anmeldeverfahrens, erfolgen auf Grundlage unserer berechtigten Interessen gem. Art. 6 Abs. 1 lit. f DSGVO. Unser Interesse richtet sich auf den Einsatz eines nutzerfreundlichen sowie sicheren Newslettersystems, das sowohl unseren geschäftlichen Interessen dient, als auch den Erwartungen der Nutzer entspricht.

Die erteilte Einwilligung zur Speicherung der Daten, der E-Mailadresse sowie deren Nutzung zum Versand des BOA-E-Mailings können Sie jederzeit widerrufen, etwa über den "Austragen"-Link im BOA-E-Mailing.

**Social Plugins**

ZEIT Online Gmbh und talentsconnect AG verwenden auf ihren BOA-Seiten auch Plugins u.a. der sozialen Netzwerke facebook.com, der Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA , Twitter.com, der Twitter Inc., 795 Folsom St., Suite 600, San Francisco CA 94107, USA sowie google +, der Google Inc., 1600 Amphitheatre Parkway Mountain View, California, 94043, USA. Sie erkennen die Plugins an dem jeweiligen Netzwerk-Logo, bspw. ergänzt um das Piktogramm einer geballten Faust mit erhobenem, nach oben zeigenden Daumen oder dem Zusatz "Empfehlung", "Like", "Kommentar" oder "Gefällt mir". Wenn Sie den "Like"-Button anklicken, übermittelt dieser verschiedene Daten an das soziale Netzwerk. Hierzu können gehören:

●      Datum und Uhrzeit des Besuchs der Website

●      URL der Website auf der sich der Besucher befindet

●      URL der Website, die der Besucher vorher besucht hatte

●      Verwendeter Browser

●      Verwendetes Betriebssystem

●      IP-Adresse des Besuchers

Sofern Sie parallel während des Besuches unserer Seite bei Facebook, Twitter oder Google + eingeloggt sind, ist nicht ausgeschlossen, dass der Anbieter den Besuch Ihrem Netzwerk-Konto zuordnet. Wenn Sie die Plugin-Funktionen nutzen (z.B. Anklicken des "Gefällt mir"-Buttons, Abgabe eines Kommentars), werden diese Informationen ebenfalls von Ihrem Browser direkt an das jeweilige soziale Netzwerk übermittelt und dort ggf. gespeichert. Zweck und Umfang der Datenerhebung und die weitere Verarbeitung und Nutzung der Daten durch die Netzwerke können den Datenschutzhinweisen von Facebook, Twitter sowie Google entnommen werden:

●      [Facebook-Pixel](https://www.zeit.de/hilfe/datenschutz#h-facebook)

●      [Twitter](https://www.zeit.de/hilfe/datenschutz#t-twitter)

●      [YouTube](https://www.zeit.de/hilfe/datenschutz#l-youtube)

●      [Google-Analytics](https://www.zeit.de/hilfe/datenschutz#j-google)

●      [Google AdWords](https://www.zeit.de/hilfe/datenschutz#j-google)

●      [Google Maps](https://www.zeit.de/hilfe/datenschutz#j-google)

**LinkedIn**

BOA Seiten nutzen Funktionen des Netzwerks LinkedIn. Anbieter ist die LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. Bei jedem Abruf einer unserer Seiten, die Funktionen von LinkedIn enthält, wird eine Verbindung zu Servern von LinkedIn aufbaut. LinkedIn wird darüber informiert, dass Sie unsere Internetseiten mit Ihrer IP-Adresse besucht haben. Wenn Sie den "Recommend-Button" von LinkedIn anklicken und in Ihrem Account bei LinkedIn eingeloggt sind, ist es LinkedIn möglich, Ihren Besuch auf unserer Internetseite Ihnen und Ihrem Benutzerkonto zuzuordnen. Wir weisen darauf hin, dass wir als Anbieter der Seiten keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch LinkedIn haben. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von LinkedIn unter:<https://www.linkedin.com/legal/privacy-policy>

**LinkedIn Analytics**

Wir verwenden auf unserem Internetauftritt "LinkedIn Analytics", einen Dienst der LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Irland (nachfolgend bezeichnet als: "LinkedIn"). LinkedIn Analytics speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt. LinkedIn Analytics verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen.

Wir verwenden LinkedIn Analytics zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unseres Internetauftritts analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Daten durch den Drittanbieter. Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können. Sie können die Erfassung der vorgenannten Informationen durch LinkedIn auch dadurch verhindern, indem Sie auf einer der nachfolgend verlinkten Webseiten ein Opt-Out-Cookie setzen:

<https://www.linkedin.com/psettings/guest-controls>

<https://optout.aboutads.info/>

<http://www.youronlinechoices.com/de/praferenzmanagement/>

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B.  https://noscript.net/ ). Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.

Informationen des Drittanbieters: LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Irland. Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen:

https://www.linkedin.com/legal/privacy-policy

**LinkedIn Marketing Solutions**

 Wir verwenden auf unserem Internetauftritt "LinkedIn Marketing Solutions", einen Dienst der LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Irland (nachfolgend bezeichnet als: "LinkedIn"). LinkedIn Marketing Solutions speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt. LinkedIn Marketing Solutions verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen.

Wir verwenden LinkedIn Marketing Solutions zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unseres Internetauftritts analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Daten durch den Drittanbieter. Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können. Sie können die Erfassung der vorgenannten Informationen durch LinkedIn auch dadurch verhindern, indem Sie auf einer der nachfolgend verlinkten Webseiten ein Opt-Out-Cookie setzen:

<https://www.linkedin.com/psettings/guest-controls>  
<https://optout.aboutads.info/>  
<http://www.youronlinechoices.com/de/praferenzmanagement/>

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B. <https://noscript.net/> oder [https://www.ghostery.com](https://www.ghostery.com/)). Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.

Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Informationen des Drittanbieters: LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Irland. Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen: <https://www.linkedin.com/legal/privacy-policy>

**XING**

BOA Seiten nutzen Funktionen des Netzwerks XING. Anbieter ist die XING AG, Dammtorstraße 29-32, 20354 Hamburg, Deutschland. Bei jedem Abruf einer unserer Seiten, die Funktionen von XING enthält, wird eine Verbindung zu Servern von XING hergestellt. Eine Speicherung von personenbezogenen Daten erfolgt dabei nach unserer Kenntnis nicht. Insbesondere werden keine IP-Adressen gespeichert oder das Nutzungsverhalten ausgewertet.

Weitere Information zum Datenschutz und dem XING Share-Button finden Sie in der Datenschutzerklärung von XING unter: <https://www.xing.com/app/share?op=data_protection>

**2. Von BOA-Recruitern angegebene Daten**

Als registrierter BOA-Recruiter wird ein Zugang zum Bewerbungsmanagement und ein Profil mit Ihren Recruitingdaten angelegt. Mit dem Zugang in das BOA-Bewerbungsmanagement können zusätzlich zur Nutzung auch die Profildaten des BOA-Recruiters verwaltet werden. Hierfür werden Vorname, Nachnamen, E-Mailadresse, sowie ein Passwort im BOA-Bewerbungsmanagement gespeichert.

Diese Daten werden benötigt, um einen User-Account als BOA-Recruiter einzurichten und zu verwalten, sowie das vollständige Angebot vom BOA-Bewerbungsmanagement nutzen zu können. Die Verarbeitung dieser personenbezogenen Daten beruht insoweit auf einem berechtigten Interesse und damit auf Art. 6 Abs. 1 lit. f) DSGVO. Bei Vertragsabschluss willigen Sie in die Verarbeitung der personenbezogenen Daten gemäß diesen Datenschutzbestimmungen ein.

Zum Zwecke der Nutzung und Ausführung des BOA-Bewerbungsmanagement bestätigt ZEIT Online daher gegenüber 22connect mittels Weitergabe Ihrer E-Mailadresse Ihre Registrierung.

Mit Ihrer Zustimmung zur Nutzung des BOA-Bewerbungsmanagement willigen Sie ein, dass  talentsconnect AG einen Abgleich Ihrer Daten mit der Registrierung bei ZEIT Online, insbesondere durch Weitergabe Ihrer E-Mailadresse von ZEIT Online an talentsconnect AG vornehmen kann und dass die von Ihnen erhobenen Daten von talentsconnect AGverarbeitet sowie an ZEIT Online übermittelt werden.

Im Übrigen erfolgt grundsätzlich keine Weitergabe der personenbezogenen Daten ohne Ihre ausdrückliche Einwilligung, soweit keine gesetzliche oder gerichtliche Verpflichtung zur Weitergabe, insbesondere an Strafverfolgungsbehörden, Finanzbehörden oder sonstige öffentliche Stellen besteht.

**Widerruf Ihrer Einwilligung zur Datenverarbeitung bei BOA**

Viele Datenverarbeitungsvorgänge sind nur mit Ihrer ausdrücklichen Einwilligung möglich. Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Dazu reicht eine formlose Mitteilung per E-Mail [email@zeit.de](mailto:email@zeit.de?subject=BOA-Widerruf). Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

**Weitergabe von Daten**

Grundsätzlich erfolgt eine Weitergabe Ihrer personenbezogenen Daten ohne Ihre ausdrückliche vorherige Einwilligung nur in den nachfolgend genannten Fällen:

Wenn es zur Aufklärung einer rechtswidrigen Plattform Nutzung dient oder für die Rechtsverfolgung erforderlich ist, werden personenbezogene Daten an die Strafverfolgungsbehörden sowie gegebenenfalls an geschädigte Dritte weitergeleitet. Dies geschieht jedoch nur dann, wenn konkrete Anhaltspunkte für ein gesetzwidriges beziehungsweise missbräuchliches Verhalten vorliegen. Eine Weitergabe kann auch dann stattfinden, wenn dies der Durchsetzung von Nutzungsbedingungen oder anderer Vereinbarungen dient. ZEIT Online GmbH ist zudem gesetzlich verpflichtet, auf Anfrage bestimmten öffentlichen Stellen Auskunft zu erteilen. Dies sind Strafverfolgungsbehörden, Behörden, die bußgeldbewährte Ordnungswidrigkeiten verfolgen und die Finanzbehörden.

Gelegentlich sind wir für die Erbringung der Dienstleistungen auf vertraglich verbundene Fremdunternehmen und externe Dienstleister angewiesen, beispielsweise in den Bereichen der Übersendung von Werbemaßnahmen (nur, sofern Sie diesen vorher explizit zugestimmt haben) sowie dem Kundenservice. In solchen Fällen werden Informationen an diese Unternehmen bzw. Einzelpersonen weitergegeben, um diesen die weitere Bearbeitung zu ermöglichen. Diese externen Serviceprovider werden von uns sorgfältig ausgewählt und regelmäßig überprüft, um sicherzugehen, dass Ihre Privatsphäre gewahrt bleibt. Die Serviceprovider dürfen die Daten ausschließlich zu den von ZEIT Online und talentsconnect AG vorgegebenen Zwecken verwenden. Die Serviceprovider werden darüber hinaus von ZEIT Online und oder talentsconnect AG vertraglich verpflichtet, Ihre Daten ausschließlich gemäß dieser Datenschutzerklärung sowie im Rahmen der DSGVO zu behandeln.

Im Rahmen der Weiterentwicklung unseres Geschäftes kann es dazu kommen, dass sich die Struktur der talentsconnect AG wandelt, indem die Rechtsform geändert wird, Tochtergesellschaften, Unternehmensteile oder Bestandteile gegründet, gekauft oder verkauft werden. Bei solchen Transaktionen werden die Kundeninformationen zusammen mit dem zu übertragenden Teil des Unternehmens weitergegeben. Bei jeder Weitergabe von personenbezogenen Daten an Dritte in dem vorbeschriebenen Umfang trägt talentsconnect AG dafür Sorge, dass dies in Übereinstimmung mit dieser Datenschutzerklärung und den einschlägigen Datenschutzgesetzen erfolgt.

**Löschung Ihrer Daten**

Teile Ihrer Daten werden aus steuerrechtlichen Gründen 10 Jahre aufbewahrt.

Wenn Sie eine Löschung Ihrer Daten wünschen, senden Sie bitte eine E-Mail an [email@zeit.de](mailto:email@zeit.de). In diesem Fall werden die personenbezogenen Daten vollständig und endgültig gelöscht. Soweit Daten aus gesetzlichen Gründen aufbewahrt werden müssen, werden diese bis zur endgültigen Löschung eingeschränkt in der Verarbeitung und somit gesperrt. Die Daten stehen einer weiteren Verwendung dann nicht mehr zur Verfügung.

**Weitere Informationen über Ihre Rechte finden Sie im**[**Abschnitt IV**](https://www.zeit.de/hilfe/datenschutz#teil-iv-ihre-rechte)

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#o-zeit-campus-berufsorientierungsangebot-boa)

**p.) ZEIT Umfragen und ZEIT Gewinnspiele**

**ZEIT Umfragen:**

Sie haben auf unserer Internetseite die Möglichkeit, an Umfragen zu verschiedenen Themen teilzunehmen. Im Rahmen dieser Umfragen, welche wir mithilfe des Programmes Typeform durchführen (weitere Infos hierzu unter [Teil III. Ziffer u)](https://www.zeit.de/hilfe/datenschutz#u-typeform), bitten wir Sie um die Beantwortung verschiedener Fragen und um Angabe von je nach Umfrage unterschiedlichen personenbezogenen Daten wie z.B. Name, E-Mailadresse, Gehaltsklasse etc. Die Angabe der persönlichen Daten ist regelmäßig freiwillig.

Geben Sie die Daten im Rahmen der Umfrage an, erteilen Sie damit gleichzeitig die Einwilligung zu dem genannten Vorgehen, die entsprechende Datenverarbeitung beruht damit auf Art. 6 Abs. 1 Satz 1 lit. a) DSGVO. Diese Einwilligung können Sie jederzeit widerrufen.

Mit der Angabe der personenbezogenen Daten stimmen Sie der eben genannten Verwendung der Daten zu, die entsprechende Datenverarbeitung beruht damit auf Art. 6 Abs. 1 Satz 1 lit. a) DSGVO. Die erteilte Einwilligung können Sie jederzeit widerrufen.

**ZEIT-Scrabble-Sommer:**

Auf unserer Internetseite haben Sie die Möglichkeit, an dem Gewinnspiel "ZEIT-Scrabble-Sommer" teilzunehmen. Zur Teilnahme am ZEIT-Scrabble-Sommer ist die Angabe der folgenden Daten notwendig: Vor- und Nachname, Adresse. Diese Angaben sind für die Teilnahme am Gewinnspiel notwendig. Die Verarbeitung dieser Daten beruht auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO.

Wir speichern Ihre Daten bis zum Ablauf des ZEIT-Scrabble-Sommers und danach bis zum Ablauf der gesetzlichen Verjährungsfrist. An der diesbezüglichen Speicherung Ihrer Daten haben wir ein berechtigtes Interesse, welches sich bereits aus Art. 17 Abs. 3 lit. e) DSGVO ergibt. Die Speicherung Ihrer Daten beruht insoweit auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Für den Fall, dass Sie einen unserer Preise gewinnen, haben wir ein berechtigtes Interesse daran, Ihren Vor- und Nachnamen in der von uns herausgegebenen Zeitung "DIE ZEIT" zu veröffentlichen. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

**ZEIT-magazin Sommerpreisrätsel:**

Auf unserer Internetseite haben Sie die Möglichkeit, an dem Gewinnspiel "ZEIT-magazin Sommerpreisrätsel" teilzunehmen. Veranstalterin des Gewinnspiels ist die Zeitverlag Gerd Bucerius GmbH & Co. KG (Zeitverlag). Wenn Sie über unsere Internetseite am Gewinnspiel teilnehmen, werden die nachstehenden Daten von uns erhoben und zur Durchführung des Gewinnspiels an den Zeitverlag weitergegeben.  Zur Teilnahme ist die Angabe der folgenden Daten notwendig: Vor- und Nachname, Adresse und Telefonnummer. Diese Angaben sind für die Teilnahme am Gewinnspiel notwendig. Die Erhebung, Weitergabe und Verarbeitung dieser Daten beruht auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO.

Der Zeitverlag speichert Ihre Daten bis zum Ablauf des "ZEITmagazin Sommer-preisrätsels" und danach bis zum Ablauf der gesetzlichen Verjährungsfrist. An der diesbezüglichen Speicherung Ihrer Daten besteht ein berechtigtes Interesse, welches sich bereits aus Art. 17 Abs. 3 lit. e) DSGVO ergibt. Die Speicherung Ihrer Daten beruht insoweit auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Für den Fall, dass Sie einen unserer Preise gewinnen, besteht ein berechtigtes Interesse daran, Ihren Vor- und Nachnamen in der von uns herausgegebenen Zeitung "DIE ZEIT" zu veröffentlichen. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#p-zeit-umfragen-und-zeit-gewinnspiele)

**q.) ZEIT Audio Skill**

Über unseren ZEIT Audio Skill für Amazon Alexa können Sie sich Inhalte der aktuellen Ausgabe der ZEIT vorlesen lassen. Die Verwendung dieses Skills ist grundsätzlich ohne Angabe personenbezogener Daten möglich.

Um das vollständige Angebot des Skills nutzen zu können, ist jedoch eine Verknüpfung Ihres ZEIT-Abo-Accounts mit Amazon erforderlich. Es ist hierbei aber technisch gewährleistet, dass keine personenbezogenen Account-Daten oder Kunden-IDs an Amazon übertragen werden. Wir nutzen hierfür den Dienstleister Auth0, Inc. (USA), der für die Verifizierung Ihrer Kundendaten gegenüber Amazon beauftragt und im Wege der Auftragsverarbeitung durch uns verpflichtet wurde.  Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Die Verwendung Ihrer Zeit-Account-Daten ist für die unbeschränkte Nutzung des Skills erforderlich. Die Datenverarbeitung beruht somit auf Art. 6 Abs. 1 lit. b) DSGVO.

Wir geben im Übrigen keine personenbezogene Daten an Amazon weiter. Amazon weist Ihnen bei Aktivierung unseres Skills eine eigene User-ID zu, die aber nicht an uns übertragen wird. Wenn Sie unseren Skill nutzen und außerhalb der für die Nutzung erforderlichen Sprachbefehle (siehe Beschreibung) personenbezogene Daten mitteilen, werden diese Informationen durch Amazon gespeichert und verarbeitet. Wir haben keinen Einfluss auf den Umfang und die Speicherung dieser personenbezogenen Daten. Informationen zum Umgang Ihrer personenbezogenen Daten durch Amazon erhalten Sie in folgender Datenschutzerklärung: <https://www.amazon.de/gp/help/customer/display.html?nodeId=3312401>

Zur Optimierung unseres Angebots, analysieren wir das Nutzerverhalten des ZEIT Audio Skills mit Hilfe von Webtrekk. Hierzu verwendet Webtrekk eine anonymisierte User-ID, die in einem Cookie gespeichert wird. Die ID wird weder mit Ihren Account-Daten der ZEIT noch der Amazon User-ID verknüpft. Durch die statistische Auswertung unseres Skills können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Daten durch Webtrekk. Die Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. f) DSGVO . Sie können dieser Form des Trackings jederzeit widersprechen, indem Sie den ZEIT Audio Skill in Ihrem Amazon Konto deaktivieren.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#q-zeit-audio-skill)

**r.) Podigee Podcast-Hosting**

Wir nutzen den Podcast-Hosting-Dienst [Podigee](https://www.podigee.com/de/) des Anbieters Podigee GmbH, Ritterstraße 2A, 10969 Berlin, Deutschland. Die Podcasts werden dabei von Podigee geladen oder über Podigee übertragen. Die Nutzung erfolgt auf Grundlage unserer berechtigten Interessen, d.h. Interesse an einer sicheren und effizienten Bereitstellung, Analyse sowie Optimierung unseres Podcastangebotes gem. Art. 6 Abs. 1 lit. f. DSGVO.  Podigee verarbeitet IP-Adressen und Geräteinformationen, um Podcast-Downloads/Wiedergaben zu ermöglichen und statistische Daten, wie z.B. Abrufzahlen zu ermitteln. Diese Daten werden vor der Speicherung in der Datenbank von Podigee anonymisiert oder pseudonymisiert, sofern Sie für die Bereitstellung der Podcasts nicht erforderlich sind. Weitere Informationen und Widerspruchsmöglichkeiten finden sich in der Datenschutzerklärung von Podigee:  <https://www.podigee.com/de/about/privacy/>.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#r-podigee-podcast-hosting)

**TEIL III: Bei der Nutzung unserer Website automatisch erhobene Daten**

Wir erheben im Falle Ihrer Einwilligung auch automatisiert Daten zu Werbezwecken. Dies geschieht, wenn Sie sich aktiv für den kostenlosen Zugang zu unserer Seite und gegen ein kostenpflichtiges Pur-Abo entschieden haben. In diesem Fall werden Nutzungsdaten für die sogenannte nutzungsbasierte Onlinewerbung getrackt, das heißt es werden Nutzungsdaten erhoben und pseudonym zu Nutzungsprofilen verarbeitet ("Werbetracking"). Dies geschieht, weil Werbetreibende für eine möglichst effiziente Online-Werbung zuverlässige Angaben benötigen, insbesondere darüber, wie viele Leser ihre Anzeigen sehen und welche Nutzer sich schätzungsweise für welche Produkte, Themen oder Angebote besonders interessieren. So kann auf Ihrem Endgerät solche Werbung ausgespielt werden, der Sie vermutlich eine größere Aufmerksamkeit schenken.

Die meisten der eingesetzten Programme die in diesem Teil beschrieben werden, verwenden zur Datenerhebung sog. "Cookies". Bei Cookies handelt es sich um kleine Textdateien, die Ihr Internetbrowser automatisch erstellt und die lokal auf Ihrem Endgerät (Computer, Tablet, Smartphone etc.) gespeichert werden, wenn Sie unsere Internetseite besuchen.

Cookies richten auf Ihrem Endgerät keinen Schaden an. Der Einsatz von Cookies dient dem Zweck, dass wir die Nutzung unseres Angebots für Sie angenehmer gestalten können. Cookies erlauben es uns beispielsweise, Sie bei einem erneuten Besuch unserer Website wiederzuerkennen, so dass Sie getätigte persönliche Einstellungen nicht wiederholen müssen.

Zudem setzen wir Cookies ein, um die Nutzung unserer Website statistisch zu erfassen und zum Zwecke der Optimierung unseres Angebotes für Sie auszuwerten oder ggf. eine gezielte Werbeausspielung zu ermöglichen. Alle Cookies werden nach einer jeweils definierten Zeitspanne, wenn sie ihren Zweck erfüllt haben, automatisch gelöscht.

Die meisten Browser akzeptieren Cookies automatisch. Sie können das Speichern von Cookies auf Ihrer Festplatte generell verhindern, indem Sie in Ihren Browser-Einstellungen "keine Cookies akzeptieren" wählen. Sie können Ihren Browser auch so einstellen, dass dieser Sie vor dem Setzen von Cookies fragt, ob Sie einverstanden sind. Schließlich können Sie auch einmal gesetzte Cookies jederzeit wieder löschen. Wie all das im Einzelnen funktioniert, entnehmen Sie bitte der Anleitung Ihres Browser-Betreibers. Bitte beachten Sie aber, dass diese Einstellungen nur für den das jeweilige Endgerät sowie den Browser gelten, auf bzw. in dem sie vorgenommen wurden.

Unter dem am Ende jeder unserer Internetseiten eingebetteten Link "[Cookies & Tracking](https://l3.evidon.com/site/5335/1772/3)" bieten wir Ihnen die Möglichkeit, transparent nachzuvollziehen, welche Cookies wir auf unserer Internetseite zur Werbeausspielung einsetzen, die Funktionsweise der einzelnen Cookies zu verstehen und nachzuvollziehen, wie ein Opt-out des jeweiligen Cookies hinterlegt werden kann.

Werbetracking setzen wir auf unserer Seite nur mit Ihrer ausdrücklichen Zustimmung ein. Daher wird vor Aufruf von zeit.de Ihre Einwilligung abgefragt. Entscheiden Sie sich aktiv für den kostenlosen Zugang zu unserer Webseite und erteilen uns damit Ihre Einwilligung zum Werbetracking, wird ein entsprechender Cookie lokal auf Ihrem Computer bzw. Endgerät gespeichert. Haben Sie diesen Cookie gelöscht oder Ihren Browser so eingestellt, dass Cookies beim Schließen automatisch aus dem Cache gelöscht werden, wird Ihre Zustimmung beim nächsten Aufruf erneut abgefragt.

Rechtsgrundlage für den Einsatz von Werbetracking und das Setzen der dafür ggf. erforderlichen Cookies ist Art. 6 Abs. 1 lit. a DSGVO.

Ihre Zustimmung zum Werbetracking können Sie jederzeit widerrufen, etwas durch Betätigung des Buttons "Zustimmung widerrufen". Einschränkungslos weiter nutzen können Sie das Angebot dann aber nur im Rahmen des Pur-Abos.

Betätigen Sie den Button "Zustimmung widerrufen" erscheint beim nächsten Laden der Webseite wieder die [vorgeschaltete Seite,](https://www.zeit.de/zustimmung) auf der Sie zwischen dem kostenlosen Zugang mit Werbetracking und dem kostenpflichtigen Pur-Zugang mit deutlich weniger Werbung und ohne Werbetracking wählen können.

Zu den von uns automatisch erhobenen Daten bzw. eingesetzten Dienste im Einzelnen:

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#teil-iii-bei-der-nutzung-unserer-website-automatisch-erhobene-daten)

**a.) Logfiles**

Beim Aufrufen unserer Website werden durch den auf Ihrem Endgerät zum Einsatz kommenden Browser automatisch Informationen an den Server unserer Website gesendet. Diese Informationen werden temporär in einem sog. Logfile gespeichert.

Es werden dabei die folgenden Informationen automatisch erfasst (IP-Adresse, Datum und Uhrzeit des Zugriffs, ggf. Name und URL der abgerufenen Datei, ggf. Website, von der aus der Zugriff erfolgt (Referrer-URL), verwendeter Browser und ggf. das Betriebssystem Ihres Rechners sowie der Name Ihres Access-Providers).

*Die IP-Adresse, also das einzige Datum, welches einen Bezug zu Ihrer Person herstellen könnte, wird unverzüglich gelöscht bzw. so anonymisiert, sodass eine Herstellung des Personenbezuges dann nicht mehr möglich ist.*

Die genannten Daten werden zu administrativen Zwecken durch uns verarbeitet sowie dazu, um Ihnen einen reibungslosen Verbindungsaufbau und eine komfortable Nutzung unserer Website zu gewährleisten sowie um sicherzustellen, dass unser System sicher und stabil arbeitet. Die Datenverarbeitung beruht auf unserem bestehenden berechtigten Interesse an der Datenverarbeitung zu den genannten Zwecken und damit auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#a-logfiles)

**b.) iq digital Werbungsvermarktung**

Die Vermarktung der Werbemittelplätze auf unserer Webseite wird durch die iq digital media marketing gmbh, Toulouser Allee 27, D-40211 Düsseldorf ("iq digital"), in unserem Auftrag und nach unserer Weisung durchgeführt. Bitte informieren Sie sich in der Datenschutzerklärung von iq digital ([https://www.iqdigital.de/service/datenschutz-nach-tcf](https://www.iqdigital.de/service/datenschutz-nach-tcf/)) über die durch iq digital eingesetzten Partner und Toolanbieter und die jeweiligen Datenverarbeitungen. In der Datenschutzerklärung von iq digital finden Sie etwa Informationen über die Empfänger von Daten, Löschfristen, Erlaubnistatbestände und detaillierte Angaben über die genaueren Zwecke der Datenverarbeitung durch jeden einzelnen Partner und Toolanbieter.

Wir haben mit iq digital eine Auftragsverarbeitungsvereinbarung zur Einhaltung der gesetzlichen Datenschutzbestimmungen geschlossen.

Wir setzen die Technologien von iq digital im Bereich des Werbetrackings nur mit Ihrer jederzeit widerruflichen Einwilligung ein, siehe <https://www.zeit.de/hilfe/datenschutz#a-zeit-de-mit-werbung-oder-zeit-de-pur>. Die entsprechende Datenverarbeitung beruht auf der Rechtsgrundlage Art. 6 Abs. 1 lit. a) DSGVO.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#b-iq-digital-werbungsvermarktung)

**c.) Messverfahren ("SZMnG") der INFOnline GmbH**

Unsere Webseite nutzt das Messverfahren ("SZMnG") der [INFOnline GmbH, Brühler Str. 9, 53119 Bonn](https://www.infonline.de/)zur Ermittlung statistischer Kennwerte über die Nutzung unserer Angebote.

Ziel der Nutzungsmessung ist es, die Anzahl der Besuche auf unserer Website, die Anzahl der Websitebesucher und deren Surfverhalten statistisch – auf Basis eines einheitlichen Standardverfahrens - zu bestimmen und somit marktweit vergleichbare Werte zu erhalten.

Für alle Digital-Angebote, die Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW – [http://www.ivw.eu](http://www.ivw.eu/)) sind oder an den Studien der Arbeitsgemeinschaft Online-Forschung e.V. (AGOF - [http://www.agof.de](http://www.agof.de/)) teilnehmen, werden die Nutzungsstatistiken regelmäßig von der AGOF und der Arbeitsgemeinschaft Media-Analyse e.V. (agma - [http://www.agma-mmc.de](http://www.agma-mmc.de/)) zu Reichweiten weiter verarbeitet und mit dem Leistungswert "Unique User" veröffentlicht sowie von der IVW mit den Leistungswerten "Page Impression" und "Visits". Diese Reichweiten und Statistiken können auf den jeweiligen Webseiten eingesehen werden.

**1. Rechtsgrundlage für die Verarbeitung**

Die Messung mittels des Messverfahrens SZMnG durch die INFOnline GmbH erfolgt mit berechtigtem Interesse nach Art. 6 Abs. 1 lit. f) DSGVO. Zweck der Verarbeitung der personenbezogenen Daten ist die Erstellung von Statistiken und die Bildung von Nutzerkategorien. Die Statistiken dienen dazu, die Nutzung unseres Angebots nachvollziehen und belegen zu können. Die Nutzerkategorien bilden die Grundlage für eine interessengerechte Ausrichtung von Werbemitteln bzw. Werbemaßnahmen. Zur Vermarktung dieser Webseite ist eine Nutzungsmessung, welche eine Vergleichbarkeit zu anderen Marktteilnehmern gewährleistet, unerlässlich. Unser berechtigtes Interesse ergibt sich aus der wirtschaftlichen Verwertbarkeit der sich aus den Statistiken und Nutzerkategorien ergebenden Erkenntnisse und dem Marktwert unserer Webseite -auch in direktem Vergleich mit Webseiten Dritter- der sich anhand der Statistiken ermitteln lässt. Darüber hinaus haben wir ein berechtigtes Interesse daran, die pseudonymisierten Daten der INFOnline, der AGOF und der IVW zum Zwecke der Marktforschung (AGOF, agma) und für statistische Zwecke (INFOnline, IVW) zur Verfügung zu stellen. Weiterhin haben wir ein berechtigtes Interesse daran, die pseudonymisierten Daten der INFOnline zur Weiterentwicklung und Bereitstellung interessengerechter Werbemittel zur Verfügung zu stellen.

**2. Art der Daten**

Die INFOnline GmbH erhebt die folgenden Daten, welche nach EU-DSGVO einen Personenbezug aufweisen:

●      IP-Adresse: Im Internet benötigt jedes Gerät zur Übertragung von Daten eine eindeutige Adresse, die sogenannte IP-Adresse. Die zumindest kurzzeitige Speicherung der IP- Adresse ist aufgrund der Funktionsweise des Internets technisch erforderlich. Die IP- Adressen werden vor jeglicher Verarbeitung um 1 Byte gekürzt und nur anonymisiert weiterverarbeitet. Es erfolgt keine Speicherung oder weitere Verarbeitung der ungekürzten IP-Adressen.

●      Einen zufällig erzeugten Client-Identifier: Die Reichweitenverarbeitung verwendet zur Wiedererkennung von Computersystemen alternativ entweder ein Cookie mit der Kennung "ioam.de", ein "Local Storage Object" oder eine Signatur, die aus verschiedenen automatisch übertragenen Informationen Ihres Browsers erstellt wird. Diese Kennung ist für einen Browser eindeutig, solange das Cookie oder Local Storage Object nicht gelöscht wird. Eine Messung der Daten und anschließende Zuordnung zu dem jeweiligen Client- Identifier ist daher auch dann möglich, wenn Sie andere Webseiten aufrufen, die ebenfalls das Messverfahren ("SZMnG") der INFOnline GmbH nutzen. Die Gültigkeit des Cookies ist auf maximal 1 Jahr beschränkt.

**3. Nutzung der Daten**

Das Messverfahren der INFOnline GmbH, welches auf dieser Webseite eingesetzt wird, ermittelt Nutzungsdaten. Dies geschieht, um die Leistungswerte Page Impressions, Visits und Clients zu erheben und weitere Kennzahlen daraus zu bilden (z.B. qualifizierte Clients). Darüber hinaus werden die gemessenen Daten wie folgt genutzt:

●      Eine sogenannte Geolokalisierung, also die Zuordnung eines Webseitenaufrufs zum Ort des Aufrufs, erfolgt ausschließlich auf der Grundlage der anonymisierten IP-Adresse und nur bis zur geographischen Ebene der Bundesländer / Regionen. Aus den so gewonnenen geographischen Informationen kann in keinem Fall ein Rückschluss auf den konkreten Aufenthaltsort eines Nutzers gezogen werden.

●      Die Nutzungsdaten eines technischen Clients (bspw. eines Browsers auf einem Gerät) werden webseitenübergreifend zusammengeführt und in einer Datenbank gespeichert. Diese Informationen werden zur technischen Abschätzung der Sozioinformation Alter und Geschlecht verwendet und an die Dienstleister der AGOF zur weiteren Reichweitenverarbeitung übergeben. Im Rahmen der AGOF-Studie werden auf Basis einer zufälligen Stichprobe Soziomerkmale technisch abgeschätzt, welche sich den folgenden Kategorien zuordnen lassen: Alter, Geschlecht, Nationalität, Berufliche Tätigkeit, Familienstand, Allgemeine Angaben zum Haushalt, Haushalts-Einkommen, Wohnort, Internetnutzung, Online-Interessen, Nutzungsort, Nutzertyp.

**4. Speicherdauer der Daten**

Die vollständige IP-Adresse wird von der INFOnline GmbH nicht gespeichert. Die gekürzte IP- Adresse wird maximal 60 Tage gespeichert. Die Nutzungsdaten in Verbindung mit dem eindeutigen Identifier werden maximal 6 Monate gespeichert.

**5. Weitergabe der Daten**

Die IP-Adresse wie auch die gekürzte IP-Adresse werden nicht weitergegeben. Für die Erstellung der AGOF-Studie werden Daten mit Client-Identifiern an die folgenden Dienstleister der AGOF weitergegeben:

●      KantarDeutschland GmbH (<https://www.kantardeutschland.de/> )

●      Ankordata GmbH & Co. KG (<http://www.ankordata.de/homepage/>)

●      Interrogare GmbH (<https://www.interrogare.de/>)

**Für ZEIT Online Apps gilt folgendes:**

Unsere Applikationen nutzen das Messverfahren ("SZMnG") der INFOnline GmbH (https://[www.INFOnline.de](http://www.infonline.de/)) zur Ermittlung statistischer Kennwerte über die Nutzung unserer Angebote. Ziel der Nutzungsmessung ist es, die Nutzungsintensität, die Anzahl der Nutzungen und Nutzer unserer Applikationen und deren Surfverhalten statistisch– auf Basis eines einheitlichen Standardverfahrens - zu bestimmen und somit marktweit vergleichbare Werte zu erhalten.  
Für alle Digital-Angebote, die Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW – [http://www.ivw.eu](http://www.ivw.eu/)) sind oder an den Studien der Arbeitsgemeinschaft Online-Forschung e.V. (AGOF – [http://www.agof.de](http://www.agof.de/)) teilnehmen, werden die Nutzungsstatistiken regelmäßig von der AGOF und der Arbeitsgemeinschaft Media-Analyse e.V. (agma – [http://www.agma-mmc.de](http://www.agma-mmc.de/)) zu Reichweiten weiter verarbeitet und mit dem Leistungswert "Unique User" veröffentlicht sowie von der IVW mit den Leistungswerten "Page Impression" und "Visits". Diese Reichweiten und Statistiken können auf den jeweiligen Webseiten eingesehen werden.

**1. Rechtsgrundlage für die Verarbeitung**

Die Messung mittels des Messverfahrens SZMnG durch die INFOnline GmbH erfolgt mit berechtigtem Interesse nach Art. 6 Abs. 1 lit. f) DSGVO.  
Zweck der Verarbeitung der personenbezogenen Daten ist die Erstellung von Statistiken zur Bildung von Nutzerkategorien. Die Statistiken dienen uns dazu, die Nutzung unseres Angebots nachvollziehen und belegen zu können. Die Nutzerkategorien bilden die Grundlage für eine interessengerechte Ausrichtung von Werbemitteln bzw. Werbemaßnahmen. Zur Vermarktung dieser Applikation ist eine Nutzungsmessung, welche eine Vergleichbarkeit zu anderen Marktteilnehmern gewährleistet, unerlässlich. Unser berechtigtes Interesse ergibt sich aus der wirtschaftlichen Verwertbarkeit der sich aus den Statistiken und Nutzerkategorien ergebenden Erkenntnisse und dem Marktwert unserer Applikation -auch in direktem Vergleich mit Applikationen Dritter-, der sich anhand der Statistiken ermitteln lässt.  
Darüber hinaus haben wir ein berechtigtes Interesse daran, die pseudonymisierten Daten der INFOnline, der AGOF und der IVW zum Zwecke der Marktforschung (AGOF, agma) und für statistische Zwecke (IVW, INFOnline) zur Verfügung zu stellen. Weiterhin haben wir ein berechtigtes Interesse daran, die pseudonymisierten Daten der INFOnline zur Weiterentwicklung und Bereitstellung interessengerechter Werbemittel zur Verfügung zu stellen.

**2. Art der Daten**

Die INFOnline GmbH erhebt die folgenden Daten, welche nach DSGVO einen Personenbezug aufweisen:

●      IP-Adresse: Im Internet benötigt jedes Gerät zur Übertragung von Daten eine eindeutige Adresse, die sogenannte IP-Adresse. Die zumindest kurzzeitige Speicherung der IP- Adresse ist aufgrund der Funktionsweise des Internets technisch erforderlich. Die IP-Adressen werden vor jeglicher Verarbeitung gekürzt und nur anonymisiert weiterverarbeitet. Es erfolgt keine Speicherung oder Verarbeitung der ungekürzten IP- Adressen.

●      Einen zufällig erzeugten Client-Identifier: Die Reichweitenverarbeitung verwendet zur Wiedererkennung von Computersystemen alternativ entweder ein Third-Party-Cookie, ein First-Party-Cookie, ein "Local Storage Object" oder eine Signatur, die aus verschiedenen automatisch übertragenen Informationen Ihres Browsers erstellt wird. Diese Kennung ist für einen Browser eindeutig, solange das Cookie oder Local Storage Object nicht gelöscht wird. Eine Messung der Daten und anschließende Zuordnung zu dem jeweiligen Client-Identifier ist daher auch dann möglich, wenn Sie andere Webseiten aufrufen, die ebenfalls das Messverfahren ("SZMnG") der INFOnline GmbH nutzen.  
Die Gültigkeit des Cookies ist auf maximal 1 Jahr beschränkt.

**3. Nutzung der Daten**

Das Messverfahren der INFOnline GmbH, welches in dieser Applikation eingesetzt wird, ermittelt Nutzungsdaten. Dies geschieht, um die Leistungswerte Page Impressions, Visits und Clients zu erheben und weitere Kennzahlen daraus zu bilden (z.B. qualifizierte Clients). Darüber hinaus werden die gemessenen Daten wie folgt genutzt:

●      Eine sogenannte Geolokalisierung, also die Zuordnung eines Webseitenaufrufs zum Ort des Aufrufs, erfolgt ausschließlich auf der Grundlage der anonymisierten IP-Adresse und nur bis zur geographischen Ebene der Bundesländer / Regionen. Aus den so gewonnenen geographischen Informationen kann in keinem Fall ein Rückschluss auf den konkreten Wohnort eines Nutzers gezogen werden.

●      Die Nutzungsdaten eines technischen Clients (bspw. eines Browsers auf einem Gerät) werden applikationsübergreifend zusammengeführt und in einer Datenbank gespeichert. Diese Informationen werden zur technischen Abschätzung der Sozioinformation Alter und Geschlecht verwendet und an die Dienstleister der AGOF zur weiteren Reichweitenverarbeitung übergeben. Im Rahmen der AGOF-Studie werden auf Basis einer zufälligen Stichprobe Soziomerkmale technisch abgeschätzt, welche sich den folgenden Kategorien zuordnen lassen: Alter, Geschlecht, Nationalität, Berufliche Tätigkeit, Familienstand, Allgemeine Angaben zum Haushalt, Haushalts-Einkommen, Wohnort, Internetnutzung, Online-Interessen, Nutzungsort, Nutzertyp.

**4. Speicherdauer der Daten**

Die vollständige IP-Adresse wird von der INFOnline GmbH nicht gespeichert. Die gekürzte IP- Adresse wird maximal 60 Tage gespeichert. Die Nutzungsdaten in Verbindung mit dem eindeutigen Identifier werden maximal 6 Monate gespeichert.

**5. Weitergabe der Daten**

Die IP-Adresse wie auch die gekürzte IP-Adresse werden nicht weitergegeben. Für die Erstellung der AGOF-Studie werden Daten mit Client-Identifiern an die folgenden Dienstleister der AGOF weitergegeben:  
Kantar Deutschland GmbH (<https://www.kantardeutschland.de/>) Ankordata GmbH & Co. KG (<http://www.ankordata.de/homepage/>) Interrogare GmbH (<https://www.interrogare.de/>)

**Widerspruchsrecht**  
Wenn Sie an der Messung nicht teilnehmen möchten, können Sie unter folgendem Link widersprechen: [https://optout.ioam.de](https://optout.ioam.de/)  
Um einen Ausschluss von der Messung zu garantieren, ist es technisch notwendig, ein Cookie zu setzen. Sollten Sie die Cookies in Ihrem Browser löschen, ist es notwendig, den Opt-Out-Vorgang unter dem oben genannten Link zu wiederholen.

Die betroffene Person hat das Recht, bei einer Datenschutzbehörde Beschwerde einzulegen.  
Weitere Informationen zum Datenschutz im Messverfahren finden Sie auf der Webseite der INFOnline GmbH ([https://www.infonline.de](https://www.infonline.de/)), die das Messverfahren betreibt, der Datenschutzwebseite der AGOF (<http://www.agof.de/datenschutz>) und der Datenschutzwebseite der IVW ([http://www.ivw.eu](http://www.ivw.eu/)).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#c-messverfahren-szmng-der-infonline-gmbh)

**d.) Webtrekk GmbH**

Zur Verbesserung und Weiterentwicklung unserer Online Seite analysieren wir statistische Kennwerte über die Nutzung unserer Angebote und Dienste. Im Rahmen Ihres Besuchs werden für unsere Entwicklungs-Abteilung nicht personenbezogene Informationen erhoben, die Ihr Browser übermittelt. Zur Erhebung dieser Daten nutzen wir die Dienste der Firma Webtrekk GmbH.

Webtrekk ermöglicht uns, statistische Daten über die Nutzung unserer Webseite zu erheben und unser Angebot entsprechend zu verbessern. Webtrekk verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unserer Webseite durch Sie ermöglichen. Die Erhebung der gewonnenen Informationen erfolgt durch einen auf unserer Webseite eingebundenen Pixel. Bei jedem Zugriff auf unsere Webseite werden die nachfolgenden Informationen erhoben und ausgewertet, die von Ihrem Webbrowser übermittelt werden:

● Name der abgerufenen konkreten Webseite

● Datum und Uhrzeit

● Webbrowser-Informationen

● Betriebssystem

● Bildschirmauflösung und Farbtiefe des Endgeräts

● Referrer URL (zuvor besuchte Seite)

● IP-Adresse

● Klicks

● eventuell Formularinhalte, z.B. in Freitextfelder eingegebene Inhalte (Name und Passwort, wird nur "ausgefüllt" oder "nicht ausgefüllt" übertragen)

Weitere Informationen zu den übermittelten Inhalten finden Sie unter <http://www.webtrekk.com/index/datenschutzerklaerung.html>.

Webtrekk speichert die IP-Adresse nur in gekürzter, anonymisierter Form. Sie wird nur zur Session-Erkennung, für die Geolokalisierung und für die Abwehr von Cyber-Attacken verwendet. Die IP-Adresse wird dann umgehend wieder gelöscht. Eine Personenbeziehbarkeit ist damit ausgeschlossen. Webtrekk setzt folgende Cookies:

● Session Cookie (für Session-Erkennung, Lebensdauer: eine Session)

● Langzeit-Cookie (zur Erkennung Neu-/Stammkunde: 6 Monate)

● Opt-out-Cookie (bei Widerspruch gegen das Tracking: 60 Monate)

Wir verwenden Webtrekk zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unserer Webseite analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können.

Durch die anonymisierte statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Daten durch Webtrekk. Die Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. f) DSGVO.

Die Bildung von pseudonymisierten Profildaten findet nur mit ihrer Einwilligung statt bzw. auf der Rechtsgrundlage Art. 6 Abs. 1 lit. a) DSGVO. Sie können der Datenspeicherung ihrer pseudonymisiert erfassten Besucherdaten widersprechen, so dass sie in Zukunft nicht mehr erfasst werden.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unserer Webseite vollumfänglich nutzen können. Sie können die Erfassung der der vorgenannten Informationen durch Webtrekk auch dadurch verhindern, indem Sie auf der nachfolgend verlinkten Webseite ein Opt-Out-Cookie setzen: <http://www.webtrekk.com/index/datenschutzerklaerung/opt-out.html>.

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen.Weitere Informationen des Drittanbieters zum Datenschutz können Sie den nachfolgenden Webseiten von Webtrekk entnehmen: <https://www.webtrekk.com/de/legal/opt-out-webtrekk/> und  <https://www.webtrekk.com/privacy-notice.html>.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#d-webtrekk-gmbh)

**e.) Meetrics GmbH**

Wir verwenden auf unserem Internetauftritt "Meetrics", einen Dienst der Meetrics GmbH, Alexanderstraße 7, 10178 Berlin, Deutschland (nachfolgend bezeichnet als: "Meetrics").

Meetrics speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt. Meetrics verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen.

Wir verwenden Meetrics zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unseres Internetauftritts analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Informationen. Die entsprechende Datenverarbeitung beruht auf  Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen: <https://www.meetrics.com/datenschutz/>

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#e-meetrics-gmbh)

**h.) Facebook**

**h.1.) Facebook Audiences Retargeting**

Auf unseren Seiten ist das Custom Audiences Retargeting-Pixel (Javascript-Code) des sozialen Netzwerks [Facebook](https://de-de.facebook.com/), 1 Hacker Way, Menlo Park, CA 94025, USA, integriert. Bei dem Besuch unserer Internetseiten wird über diesen Code eine Verbindung zwischen Ihrem Browser und dem Facebook-Server hergestellt, so dass Facebook die Information erhält, dass Sie mit Ihrer IP-Adresse unsere Seite besucht haben. Das Verfahren dient dazu, dass wir auf Facebook an ein definiertes Publikum Werbeanzeigen ausspielen können. Wir weisen darauf hin, dass wir als Anbieter der Seite keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch Facebook erhalten.

Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B. <https://noscript.net/> oder [https://www.ghostery.com](https://www.ghostery.com/)). Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.Falls Sie keine Datenerfassung via Custom Audiences wünschen, können Sie Custom Audiences hier deaktivieren <https://www.facebook.com/ads/website_custom_audiences>.

Wir setzen Facebook Audiences Retargeting nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen zu den erhobenen Daten und dem Datenschutz finden Sie in der Datenrichtlinie von Facebook unter <https://www.facebook.com/about/privacy/>.

**h.2.) Facebook Connect**

Wir verwenden auf unserer Webseite "Facebook Connect", einen Dienst der Facebook Inc., 1601 S California Ave, Palo Alto, California 94304, USA (nachfolgend bezeichnet als: "Facebook"). Facebook Connect erleichtert die Registrierung für Dienste im Internet. Statt der Nutzung einer Registrierungsmaske unserer Webseite können Sie Ihre Login-Daten für Facebook eingeben und dann unser Angebot nutzen. Durch den Einsatz von "Facebook Connect" baut Ihr Webbrowser automatisch eine direkte Verbindung mit dem Server von Facebook auf. Zur Anmeldung werden Sie auf die Seite von Facebook weitergeleitet. Dort können Sie sich mit ihren Nutzungsdaten anmelden. Hierdurch wird Ihr Nutzerkonto bei Facebook mit unserem Dienst verknüpft. Wir haben keinen Einfluss auf den Umfang und die weitere Verwendung von Daten, die durch den Einsatz von Facebook Connect durch Facebook erhoben werden. Nach unserem Kenntnisstand erhält Facebook die Information, dass Sie den entsprechenden Teil unserer Webseite aufgerufen oder eine Anzeige von uns angeklickt haben. Wenn Sie über ein Nutzerkonto bei Facebook verfügen und registriert sind, kann Facebook den Besuch Ihrem Nutzerkonto zuordnen. Selbst wenn Sie nicht bei Facebook registriert sind bzw. sich nicht eingeloggt haben, besteht die Möglichkeit, dass der Facebook Ihre IP-Adresse und ggf. weitere Identifizierungsmerkmale in Erfahrung bringt und speichert.

Wir verwenden Facebook Connect, um Ihnen den Registrierungs- und Anmeldevorgang zu erleichtern und diesen zu verkürzen.

Wir setzen Facebook Connect nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Eine Verarbeitung vorstehender Informationen durch Facebook können Sie dadurch verhindern, dass Sie unsere Registrierungsmaske verwenden und Facebook Connect nicht nutzen.

Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite von Facebook entnehmen: <https://www.facebook.com/about/privacy>

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#h-facebook)

**i.) CeleraOne**

Zudem wird ein Dienst der CeleraOne GmbH, Usedomer Straße 4, 13355 Berlin genutzt, mit dem Cookies in den Browsern der Nutzer gespeichert werden. So kann festgestellt werden, wie oft einzelne Nutzer welche unserer Internetseiten besuchen. Die Daten werden ausschließlich auf Servern in der EU oder dem Europäischen Wirtschaftsraum gespeichert und analysiert, auf die nur ZEIT ONLINE zugreifen kann. Sie können die Speicherung der Cookies durch eine entsprechende Einstellung Ihrer Browser-Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website vollumfänglich werden nutzen können.

Sofern Sie registrierter Nutzer sind und sich bei ZEIT ONLINE angemeldet haben, wird an CeleraOne eine User ID übermittelt, die für CeleraOne keinen Rückschluss auf Ihre personenbezogenen Daten ermöglicht. Sie können die Übermittlung dieser User ID beenden, indem Sie die Löschung Ihres Benutzerkontos per E-Mail an [email@zeit.de](mailto:email@zeit.de?subject=L%C3%B6schanfrage%20Benutzerkonto%20ZEIT%20ONline) beantragen. Mit der Löschung Ihres Kontos verzichten Sie auf die Nutzung der registrierungspflichtigen Angebote.

An der Erlangung dieser Daten haben wir ein unternehmerisches Interessen, weil die Erlangung dieser Daten uns hilft, unser Internetangebot auf Ihre Bedürfnisse angepasst auszuspielen. Die Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. b) DSGVO. Die Speicherdauer beträgt 10 Jahre.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#i-celeraone)

**j.) Google**

**j.1) Google Analytics**

Wir verwenden auf unserern Webseiten und im Bereich <https://zeit.immowelt.de/> "Google Analytics", einen Webanalysedienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google verwendet Cookies, also kleine Textdateien, die auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unserer Webseite durch Sie ermöglichen. Die durch das Cookie erzeugten Informationen über die Benutzung unserer Webseite werden in der Regel an einen Server von Google in den USA übertragen und dort gespeichert. Wenn auf der Webseite eine Anonymisierung der durch das Cookie zu übermittelnden IP-Adresse aktiviert ist ("IP-Anonymisierung" ), wird Ihre IP-Adresse von Google innerhalb von Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zuvor gekürzt. Nur in Ausnahmefällen wird die volle IP-Adresse an einen Server von Google in den USA übertragen und dort gekürzt. Google wird diese Informationen benutzen, um in unserem Auftrag Ihre Nutzung unserer Webseite auszuwerten, Reports über die Webseitennutzung zusammenzustellen und weitere mit der Webseitennutzung und der Internetnutzung verbundene Dienstleistungen gegenüber uns zu erbringen. Dabei können aus den verarbeiteten Daten pseudonyme Nutzungsprofile erstellt werden. Die Bildung von Profildaten findet nur mit ihrer Einwilligung statt, d.h. auf der Rechtsgrundlage Art. 6 Abs. 1 lit. a) DSGVO. Die bei der Verwendung von Google Analytics übermittelte IP-Adresse wird nicht mit anderen Daten von Google zusammengeführt.

Wir verwenden Google Analytics nur mit der zuvor beschriebenen aktivierten IP-Anonymisierung. Das bedeutet, Ihre IP-Adresse wird von Google nur gekürzt weiterverarbeitet. Ein Personenbeziehbarkeit kann dadurch ausgeschlossen werden.

Wir verwenden Google Analytics auch zu dem Zweck, die Nutzung unserer Webseite analysieren und einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die anonymisierte statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Daten durch Google, diese beruht insoweit auf Art. 6 Abs. 1 lit. f) DSGVO.

Sie können das Speichern der von Google Analytics erzeugten Cookies durch Vornahme entsprechender Einstellungen Ihres Webbrowsers verhindern. Wir weisen Sie insoweit darauf hin, dass Sie in diesem Fall möglicherweise nicht sämtliche Funktionen unserer Webseite nutzen können. Wenn Sie die Erhebung der durch das Cookie erzeugten und auf Ihr Nutzerverhalten bezogenen Daten (auch Ihrer IP-Adresse) sowie die Verarbeitung dieser Daten durch Google verhindern wollen, können Sie das unter dem nachfolgenden Link verfügbare Webbrowser-Plugin herunterladen und installieren: <https://tools.google.com/dlpage/gaoptout?hl=de>.

Um Google zur Auftragsverarbeitung der übermittelten Daten nur entsprechend unserer Weisungen und zur Einhaltung der geltenden Datenschutzvorschriften zu verpflichten, haben wir mit Google einen Auftragsverarbeitungsvertrag abgeschlossen. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen zur Datennutzung durch Google, zu Einstellungs- und Widerspruchsmöglichkeiten sowie zum Datenschutz können Sie den nachfolgenden Webseiten von Google entnehmen:

● Nutzerbedingungen: <http://www.google.com/analytics/terms/de.html>

● Übersicht zum Datenschutz: <http://www.google.com/intl/de/analytics/learn/privacy.html>

● Datenschutzerklärung: <http://www.google.de/intl/de/policies/privacy>

● Datennutzung durch Google bei Ihrer Nutzung von Websites oder Apps unserer Partner: <https://www.google.com/intl/de/policies/privacy/partners>

● Datennutzung zu Werbezwecken: <http://www.google.com/policies/technologies/ads>

● Einstellungen zu personalisierter Werbung durch Google: <http://www.google.de/settings/ads>

**j.2) Google AdWords**

Wir verwenden auf unserer Webseite "Google Adwords", einen Dienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google Adwords ermöglicht uns, mit Hilfe von Werbemitteln (sogenannten Google Adwords) auf externen Webseiten auf unsere attraktiven Angebote aufmerksam zu machen. Dadurch können wir ermitteln, wie erfolgreich einzelne Werbemaßnahmen sind. Diese Werbemittel werden durch Google über sogenannte "Ad Server" ausgeliefert. Wir verwenden hierfür sog. Ad Server Cookies, durch die bestimmte Parameter zur Erfolgsmessung, wie Einblendung der Anzeigen oder Klicks durch die Nutzer, gemessen werden können. Sofern Sie über eine Google-Anzeige auf unsere Webseite gelangen, wird von Google Adwords ein Cookie auf ihrem PC gespeichert. Diese Cookies verlieren in der Regel nach 30 Tagen ihre Gültigkeit. Sie sollen nicht dazu dienen, Sie persönlich zu identifizieren. Zu diesem Cookie werden in der Regel als Analyse-Werte folgende Informationen gespeichert: Unique Cookie-ID, Anzahl Ad Impressions pro Platzierung (Frequency), letzte Impression (relevant für Post-View-Conversions), Opt-out-Informationen (Markierung, dass der Nutzer nicht mehr angesprochen werden möchte). Diese Cookies ermöglichen Google eine Wiedererkennung Ihres Webbrowsers. Sofern ein Nutzer bestimmte Seiten der Webseite eines Adwords-Kunden besucht und das auf seinem Computer gespeicherte Cookie noch nicht abgelaufen ist, können Google und der Kunde erkennen, dass der Nutzer auf die Anzeige geklickt hat und zu dieser Seite weitergeleitet wurde. Jedem Adwords-Kunden wird ein anderes Cookie zugeordnet. Cookies können somit nicht über die Webseiten von Adwords-Kunden nachverfolgt werden. Wir selbst erheben und verarbeiten in den genannten Werbemaßnahmen keine personenbezogenen Daten. Wir erhalten von Google lediglich statistische Auswertungen zur Verfügung gestellt. Anhand dieser Auswertungen können wir erkennen, welche der eingesetzten Werbemaßnahmen besonders effektiv sind. Weitergehende Daten aus dem Einsatz der Werbemittel erhalten wir nicht, insbesondere können wir die Nutzer nicht anhand dieser Informationen identifizieren. Aufgrund der eingesetzten Marketing-Tools baut Ihr Browser automatisch eine direkte Verbindung mit dem Server von Google auf. Wir haben keinen Einfluss auf den Umfang und die weitere Verwendung der Daten, die durch den Einsatz von Google AdWords durch Google erhoben werden. Nach unserem Kenntnisstand erhält Google die Information, dass Sie den entsprechenden Teil unserer Webseite aufgerufen oder eine Anzeige von uns angeklickt haben. Wenn Sie über ein Nutzerkonto bei Google verfügen und registriert sind, kann Google den Besuch Ihrem Nutzerkonto zuordnen. Selbst wenn Sie nicht bei Google registriert sind bzw. sich nicht eingeloggt haben, besteht die Möglichkeit, dass der Google Ihre IP-Adresse in Erfahrung bringt und speichert.

Wir verwenden Google AdWords zu Marketing- und Optimierungszwecken, insbesondere um für Sie relevante und interessante Anzeigen zu schalten, die Berichte zur Kampagnenleistung zu verbessern und eine faire Berechnung von Werbekosten zu erreichen.

Wir setzen Google Ad Words nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unserer Webseite vollumfänglich nutzen können. Die Verhinderung der Speicherung von Cookies ist auch dadurch möglich, dass Sie Ihren Webbrowser so einstellen, dass Cookies von der Domain "www.googleadservices.com" blockiert werden (<https://www.google.de/settings/ads>). Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Zudem können Sie interessenbezogene Anzeigen über den Link <http://www.aboutads.info/choices> deaktivieren. Wir weisen Sie darauf hin, dass auch diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender)[.](https://www.zeit.de/hilfe/datenschutz#teil-i-allgemeines)

Weitere Informationen zur Datennutzung durch Google, zu Einstellungs- und Widerspruchsmöglichkeiten sowie zum Datenschutz können Sie den nachfolgenden Webseiten von Google entnehmen:

● Datenschutzerklärung: <http://www.google.de/intl/de/policies/privacy>

● Google Website-Statistiken: <https://services.google.com/sitestats/de.html>

**j.3) Google AdSense**

Wir verwenden auf unserer Webseite "Google AdSense", einen Online-Werbedienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google AdSense verwendet unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden. Google nutzt hierfür einen Web Beacon, um das Cookie auf Ihrem Endgerät zu setzen. Ihre Daten werden in die USA übertragen und dort ausgewertet. Wenn Sie mit Ihrem Google-Account eingeloggt sind, können Ihre Daten diesem direkt zugeordnet werden. Wenn Sie die Zuordnung mit Ihrem Google-Profil nicht wünschen, müssen Sie sich ausloggen. Es ist möglich, dass diese Daten an Vertragspartner von Google an Dritte und Behörden weitergegeben werden.

Wir verwenden Google AdSense zu Marketing- und Optimierungszwecken, insbesondere um für Sie relevante und interessante Anzeigen zu schalten, die Berichte zur Kampagnenleistung zu verbessern oder um zu vermeiden, dass Sie die gleichen Anzeigen mehrmals sehen.

Wir setzen Google AdSence nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unserer Webseite vollumfänglich nutzen können. Die Verhinderung der Speicherung von Cookies ist auch durch Deaktivierung der interessenbezogenen Anzeigen bei Google über den Link <http://www.google.de/ads/preferences> möglich. Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Zudem können Sie interessenbezogene Anzeigen über den Link <http://www.aboutads.info/choices> deaktivieren. Wir weisen Sie darauf hin, dass auch diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Soweit Sie die Webbrowser Firefox, Internetexplorer oder Google Chrome verwenden, können Sie unter dem nachfolgenden Link das Setzen der Cookies dauerhaft deaktivieren: <http://www.google.com/settings/ads/plugin>. Wir weisen Sie auch insoweit darauf hin, dass Sie in diesem Fall gegebenenfalls nicht alle Funktionen unserer Webseite vollumfänglich nutzen können.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen zur Datennutzung durch Google, zu Einstellungs- und Widerspruchsmöglichkeiten sowie zum Datenschutz können Sie den nachfolgenden Webseiten von Google entnehmen:

● Datenschutzerklärung: <http://www.google.de/intl/de/policies/privacy>

● Datenschutzbedingungen für Werbung: <http://www.google.de/intl/de/policies/technologies/ads>

**j.4) Google Dynamic Remarketing**

Wir verwenden auf unserer Webseite "Google Dynamic Remarketing", einen Dienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google")). Google Dynamic Remarketing ermöglicht uns, Ihnen nach Besuch unserer Webseite bei Ihrer weiteren Internetnutzung unsere Werbeanzeigen einzublenden. Dies erfolgt mittels in Ihrem Browser gespeicherter Cookies, über die Ihr Nutzungsverhalten bei Besuch verschiedener Webseiten durch Google erfasst und ausgewertet wird. So kann von Google Ihr vorheriger Besuch unserer Webseite festgestellt werden. Eine Zusammenführung der im Rahmen des Remarketings erhobenen Daten mit Ihren personenbezogenen Daten, die ggf. von Google gespeichert werden, findet nach Aussage von Google nicht statt. Insbesondere wird laut Google beim Remarketing eine Pseudonymisierung eingesetzt.

Wir verwenden Google Dynamic Remarketing zu Marketing- und Optimierungszwecken, insbesondere um für Sie relevante und interessante Anzeigen zu schalten, die Berichte zur Kampagnenleistung zu verbessern und eine faire Berechnung von Werbekosten zu erreichen. Wir setzen Google Dynamic Remarkting nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unserer Webseite vollumfänglich nutzen können. Die Verhinderung der Speicherung von Cookies ist auch dadurch möglich, dass Sie Ihren Webbrowser so einstellen, dass Cookies von der Domain "www.googleadservices.com" blockiert werden (<https://www.google.de/settings/ads>). Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Zudem können Sie interessenbezogene Anzeigen über den Link <http://www.aboutads.info/choices> deaktivieren. Wir weisen Sie darauf hin, dass auch diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen zur Datennutzung durch Google, zu Einstellungs- und Widerspruchsmöglichkeiten sowie zum Datenschutz können Sie den nachfolgenden Webseiten von Google entnehmen:

● Datenschutzerklärung: <http://www.google.de/intl/de/policies/privacy>

● Google Website-Statistiken: <https://services.google.com/sitestats/de.html>

**j.5) Google Publisher Tags**

Wir verwenden auf unserem Internetauftritt "Google Publisher Tags ", einen Dienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt. Google verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen.

Wir verwenden Google Publisher Tags zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unseres Internetauftritts analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten.

Wir setzen Google Pubisher Tags nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können. Sie können die Erfassung der vorgenannten Informationen durch Google auch dadurch verhindern, indem Sie auf einer der nachfolgend verlinkten Webseiten ein Opt-Out-Cookie setzen:

● <https://optout.networkadvertising.org/>

● <https://optout.aboutads.info/>

● <https://www.youronlinechoices.com/de/praferenzmanagement/>

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B. <https://noscript.net/> oder [https://www.ghostery.com](https://www.ghostery.com/)). Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen: <https://www.google.com/intl/de/policies/privacy/>

**j.6) Google Safeframe**

Wir verwenden auf unserem Internetauftritt "Google Safeframe", einen Dienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google Safeframe speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt. Google Safeframe verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen.

Wir verwenden Google Safeframe zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unseres Internetauftritts analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten.

Wir setzen Google Safeframe nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können. Sie können die Erfassung der vorgenannten Informationen durch Google auch dadurch verhindern, indem Sie auf einer der nachfolgend verlinkten Webseiten ein Opt-Out-Cookie setzen:

● <https://www.google.de/settings/ads>

● <https://optout.networkadvertising.org/>

● <https://optout.aboutads.info/>

● <https://www.youronlinechoices.com/de/praferenzmanagement/>

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B. <https://noscript.net/> oder [https://www.ghostery.com](https://www.ghostery.com/)). Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen: <https://www.google.com/intl/de/policies/>

**j.7) Google Tag Manager**

Wir verwenden auf unserer Webseite "Google Tag Manager", einen Dienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google Tag Manager ermöglicht uns als Vermarkter Webseiten-Tags über eine Oberfläche verwalten zu können.

Das Tool Google Tag Manager, welches die Tags implementiert, ist eine cookielose Domain und erfasst selbst keine personenbezogenen Daten. Google Tag Manager sorgt für die Auslösung anderer Tags, die ihrerseits unter Umständen Daten erfassen. Google Tag Manager greift nicht auf diese Daten zu. Wenn auf Domain- oder Cookie-Ebene eine Deaktivierung vorgenommen wurde, bleibt diese für alle Tracking-Tags bestehen, die mit Google Tag Manager implementiert werden.

Hierin liegt unser berechtigtes Interesse. Sofern überhaupt von einer personenbezogenen Datenverarbeitung beim Einsatz von Google Tag Manager ausgegangen werden könnte beruht diese auf Art. 6 Abs. 1 lit. f) DSGVO.

Weitere Informationen zum Datenschutz können Sie den nachfolgenden Webseiten von Google entnehmen:

● Datenschutzerklärung: <http://www.google.de/intl/de/policies/privacy>

● FAQ Google Tag Manager: <https://www.google.com/intl/de/tagmanager/faq.html>

● Nutzungsbedingungen Google Tag Manager: <https://www.google.com/intl/de/tagmanager/use-policy.html>

**j.8) Google (Invisible) reCAPTCHA**

Wir verwenden auf unserem Internetauftritt "Google (Invisible) reCAPTCHA", einen Dienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Google (Invisible) reCAPTCHA speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt.  
Google (Invisible) reCAPTCHA verwendet hierfür unter anderem Cookies,  also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen. Wir verwenden Google (Invisible) reCAPTCHA zur Prüfung, ob die Eingabe durch einen Menschen oder missbräuchlich durch automatisierte,  maschinelle Verarbeitung erfolgt.

Hierin liegt auch unser berechtigtes Interesse an der Verarbeitung der vorstehenden Daten durch den  Drittanbieter. Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

Die im Rahmen von Google (Invisible) reCAPTCHA übermittelte IP-Adresse wird nicht mit anderen Daten von Google zusammengeführt,  außer Sie sind zum Zeitpunkt der Nutzung von Google (Invisible) reCAPTCHA bei Ihrem Google-Account angemeldet. Wenn Sie diese Übermittlung und Speicherung von Daten über Sie und Ihr Verhalten auf  
unserer Webseite durch Google unterbinden wollen, müssen Sie sich bei Google ausloggen und zwar bevor Sie unsere Seite besuchen bzw. Google (Invisible) reCAPTCHA benutzen.  
Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den  Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres  Internetauftritts vollumfänglich nutzen können. Sie können die Erfassung der vorgenannten Informationen durch Google auch dadurch verhindern,  indem Sie auf einer der nachfolgend verlinkten Webseiten ein Opt-Out-Cookie setzen:

●      <https://www.google.de/settings/ads>

●      [http://optout.networkadvertising.org/](https://optout.networkadvertising.org/)

●      [http://optout.aboutads.info/](https://optout.aboutads.info/)

●      [http://www.youronlinechoices.com/de/praferenzmanagement/](https://www.youronlinechoices.com/de/praferenzmanagement/)

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn  Sie Ihre Cookies löschen. Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten  verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B. <https://noscript.net/> oder [https://www.ghostery.com](https://www.ghostery.com/)).  
 Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Informationen des Drittanbieters: Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Weitere Informationen des  Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen: <https://www.google.com/intl/de/policies/>

**j.9) Google Maps**

Wir verwenden auf unserer Webseite das Angebot von "Google Maps", einem Online-Kartendienst der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (nachfolgend bezeichnet als: "Google"). Dadurch können wir Ihnen interaktive Karten  direkt in der Webseite anzeigen und ermöglichen Ihnen die komfortable Nutzung der Karten-Funktion. Durch Ihren Besuch auf unserer Webseite erhält Google die Information, dass Sie die entsprechende Unterseite unserer Webseite aufgerufen haben. Dabei wird Ihre IP-Adresse  übermittelt. Dies erfolgt unabhängig davon, ob Google ein Nutzerkonto  
bereitstellt, über das Sie eingeloggt sind, oder ob kein Nutzerkonto besteht. Wenn Sie bei Google eingeloggt sind, werden Ihre Daten direkt Ihrem Konto zugeordnet. Wenn Sie die Zuordnung mit Ihrem Profil bei Google nicht wünschen, müssen Sie sich vorab ausloggen. Google speichert Ihre Daten als Nutzungsprofile und nutzt sie für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung der Webseite. Eine solche Auswertung erfolgt insbesondere (selbst für nicht eingeloggte  
Nutzer) zur Erbringung von bedarfsgerechter Werbung und um andere Nutzer über Ihre Aktivitäten auf unserer Webseite zu informieren.

Wir verwenden Google Maps, um Ihnen interaktive Karten von Google Maps anzeigen zu können und so Ihnen ein besseres Nutzungserlebnis unserer Webseite zu ermöglichen.

Google Maps ist im "erweiterten Datenschutz-Modus" eingebunden, d.h. dass keine Daten über Sie als Nutzer an Google Maps übertragen werden, wenn Sie die Maps nicht abspielen. Erst wenn Sie die Maps anzeigen lassen, wird an den Google-Server übermittelt, welche unserer Internetseiten Sie besucht haben.

Wir setzen Google Maps nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Ihnen steht ein Widerspruchsrecht zu gegen die Bildung dieser Nutzerprofile, wobei Sie sich hierfür an Google wenden müssen.

Bei der Nutzung von Google-Diensten kann eine Übermittlung der verarbeiteten Daten an die in den USA ansässige Google LLC (USA) durch uns nicht ausgeschlossen werden. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer  Verarbeitung durch den Plug-in-Anbieter erhalten Sie in den   
Datenschutzerklärungen des Anbieters. Dort erhalten Sie auch weitere  
Informationen zu Ihren diesbezüglichen Rechten und  
Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre: <http://www.google.de/intl/de/policies/privacy>

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#j-google)

**k.) Adtriba**

Unsere Webseite nutzt das Messverfahren der [AdTriba GmbH, Veilchenweg 26b, 22529 Hamburg](https://www.adtriba.com/)zur Ermittlung statistischer Kennwerte über die Nutzung unserer Angebote.

Zweck dieser Messung ist es, die werblichen Kontaktpunkte der Nutzer zu erfassen und darauf basierend die Angebotspräsentation und -intensität zu optimieren. An der Erlangung dieser Daten haben wir ein unternehmerisches Interessen, weil die Erlangung dieser Daten uns hilft, unsere Angebote anhand des Nutzerverhaltens fortzuentwickeln und stetig zu verbessern.

Wir setzen Adtriba nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die AdTriba GmbH erhebt und verarbeitet Daten nach deutschem Datenschutzrecht. Durch technische und organisatorische Maßnahmen wird sichergestellt, dass einzelne Nutzer zu keinem Zeitpunkt identifiziert werden können. Daten, die einen Bezug zu einer bestimmten, identifizierbaren Person haben, werden unverzüglich anonymisiert.

Konkret werden folgende Informationen gespeichert:

- IP-Address (pseudonymisier)

- Nutzerdaten (Browser, Betriebssystem, Device Informationen)

Wenn Sie an der Messung nicht teilnehmen möchten, können Sie unter folgendem Link widersprechen: <https://privacy.adtriba.com/>, dort befindet sich ein Button, der einen Cookie setzt, welche die Messung unterbindet. Durch Löschen des Opt-Out Cookies können Sie erneut an der anonymen Messung teilnehmen.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#k-adtriba)

**l.) YouTube**

Wir nutzen für die Einbindung von Videos u.a. den Anbieter YouTube. YouTube wird betrieben von YouTube, LLC mit Hauptsitz in 901 Cherry Ave., San Bruno, CA 94066, USA. YouTube wird vertreten durch die Google LLC. mit Sitz in 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

Wenn Sie die Internetseite, auf welcher das YouTube Plugin eingebunden ist aufrufen, wird zur Videodarstellung eine Verbindung zu den YouTube-Servern hergestellt. Hierdurch wird an den YouTube-Server übermittelt, welche unserer Internetseiten Sie besucht haben.

Youtube ist im "erweiterten Datenschutz-Modus" eingebunden, d.h. dass keine Daten über Sie als Nutzer an YouTube übertragen werden, wenn Sie die Videos nicht abspielen. Erst wenn Sie die Videos abspielen, wird an den YouTube-Server übermittelt, welche unserer Internetseiten Sie besucht haben.

Sind Sie dabei als Mitglied bei YouTube eingeloggt, ordnet YouTube diese Informationen Ihrem persönlichen Benutzerkonto zu. Bei Nutzung des Plugins, wie z.B. durch Anklicken des Start-Buttons eines Videos, wird diese Information ebenfalls Ihrem Benutzerkonto zugeordnet. Sie können diese Zuordnung verhindern, indem Sie sich vor der Nutzung unserer Internetseite aus Ihrem YouTube-Benutzerkonto sowie anderen Benutzerkonten der Firma YouTube LLC und Google LLC. abmelden und die entsprechenden Cookies der Firmen löschen.

Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch YouTube erhalten Sie in der Datenschutzerklärung. Dort erhalten Sie auch weitere Informationen zu Ihren Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre: [www.google.de/intl/de/policies/privacy](https://www.google.de/intl/de/policies/privacy). Google verarbeitet Ihre personenbezogenen Daten auch in den USA. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Wir setzen YouTube nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#l-youtube)

**m.) Brightcove**

Zur Integration von Videos nutzen wir die Dienste von Brightcove Inc.,290 Congress Street, Boston, MA 02210, USA, ein führender globaler Anbieter von Clouddiensten für Videos.

Die Brightcove-Technologien werden unter anderem eingesetzt, um Ihnen auf Ihre persönlichen Interessen ausgerichtete Videos zu empfehlen und die Zugriffe der Nutzer auf den bereitgestellten Videocontent zu analysieren, um so die Attraktivität und Funktionalität der Webseite zu verbessern. Hierzu verwendet Brightcove Cookies und erhebt gerätebezogene Daten (z.B. Browserinformationen), unter anderem auch die IP-Adressen der Nutzer, die auf den bereitgestellten Videocontent zugreifen. Diese werden unmittelbar nach Abruf pseudonymisiert und nicht personalisiert gespeichert. Personenbezogene Daten der Nutzer werden von Brightcove grundsätzlich nicht gespeichert. Sollten Sie Videos über E-Mail mit Ihren Freunden teilen, werden die so von Ihnen mitgeteilten und gespeicherten E-Mail-Adressen automatisch wieder gelöscht.

Die Datenverarbeitung beruht auf unserem sich aus den Verarbeitungszwecken ergebenden unternehmerischen Interessen und beruht auf Art. 6 Abs. 1 lit. f) DSGVO. Wenn Sie Brightcove nicht nutzen wollen finden Sie nähere Informationen zur Deaktivierung unter:

<https://support.brightcove.com/brightcove-player-cookies>

[https://support.brightcove.com/de/video-cloud-studio-cookies.](https://support.brightcove.com/de/video-cloud-studio-cookies)

Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#m-brightcove)

**n.) Outbrain (ehemalig Ligatus)**

Diese Seite verwendet Behavioral Targeting der Firma Outbrain in gemeinsamer Verantwortung mit ZEIT Online GmbH. Outbrain bedeutet Outbrain Inc., ein Unternehmen nach dem Recht von Delaware, USA, mit Hauptsitz in New York, und dessen verbundene Tochterunternehmen.

Outbrain Inc., 39 West 13th Street, 3rd floor, New York, NY 10011

Outbrains Mission ist es, für Nutzer relevante Empfehlungen anhand ihrer Interessen bereitzustellen. Zu diesem Zweck schließt Outbrain Vereinbarungen mit:

●      Online-Publishern und Partnern, die ihren Lesern relevanten Content empfehlen wollen (dabei handelt es sich um Outbrain Engage); und

●      Werbetreibenden, die erreichen wollen, dass Leser ihren Content ansehen (hierbei handelt es sich um Outbrain Amplify).

Kontaktanfragen richten Sie bitte an [PrivacyQuestions@outbrain.com](mailto:PrivacyQuestions@outbrain.com) oder auf postalischem Weg an Outbrain Inc., 39 West 13th Street, 3rd floor, New York, NY 10011, Attn: Privacy Questions / Datenschutzanfrage. Sollte Outbrain Ihre Fragen oder Anliegen nicht zu Ihrer Zufriedenheit beantworten, können Sie sich auch an folgende Ansprechpartner wenden, um Rat oder Unterstützung zu erhalten bzw. Beschwerden vorzubringen:

●      Outbrains externen Datenschutzbeauftragten: ePrivacy GmbH, vertreten durch Prof. Dr. Christoph Bauer. Die ePrivacy GmbH können Sie direkt erreichen unter [privacy@eprivacy.eu](mailto:privacy@eprivacy.eu) und/oder

●      den Information Commissioner’s Officer, die für Outbrain zuständige federführende Aufsichtsbehörde in den europäischen Ländern.

Betroffene Personen: Nutzer die mit dem Outbrain-Widget über Outbrains netzwerk von Publishern interagieren.

Zweck des Trackings: Outbrain sammelt Informationen zum Nutzerverhalten, um personalisierte Empfehlungen anbieten zu können.

Verarbeitung personenbezogener Daten: Es werden Cookie IDs, User IDs und IP-Adressen in gekürzter Form (nicht personenbezogen) verarbeitet.

Speicherdauer: Outbrain speichert einzelne Daten maximal 13 Monate im Profil eines Nutzers.

Outbrain ist im "erweiterten Datenschutz-Modus" eingebunden, d.h. dass keine Daten über Sie als Nutzer an Outbrain übertragen werden, wenn Sie die Embedds nicht zulassen. Erst wenn      die Inhalte      Ihrer Zustimmung eingebunden sind, wird an den Outbrain-Server übermittelt, welche unserer Internetseiten Sie besucht haben.

Möglichkeit zur Unterbindung der Verarbeitung (Opt-out): <https://my.outbrain.com/recommendations-settings/home>

Datenübertragungen außerhalb der EU/des EWR Wenn Outbrain personenbezogene Daten aus dem Europäischen Wirtschaftsraum in andere Länder übertragen, deren geltende Gesetze nicht über dasselbe Datenschutzniveau wie in den europäischen Gebieten verfügen, sorgt Outbrain durch eigene Maßnahmen für ein geeignetes Datenschutzniveau. Für Ihre Daten gelten somit weiterhin Ihre Rechte und Ihr Datenschutz. Beispielsweise verwendet Outbrain anerkannte Vertragsklauseln und weitere Maßnahmen, durch die für den Schutz Ihrer personenbezogenen Daten durch die Empfänger gesorgt ist. Weitergabe von Daten: Zusätzlich zu der beschriebenen Offenlegung Ihrer personenbezogenen Daten der einzelnen Nutzerarten legen wir personenbezogene Daten unter Umständen wie folgt offen:

●      Innerhalb der durch Outbrain kontrollierten Unternehmensgruppe aus internen Gründen, vorrangig für geschäftliche und betriebliche Zwecke;

●      Bei einem Geschäftsübergang, wie einer Fusion, dem Erwerb durch ein anderes Unternehmen oder dem teilweisen oder vollständigen Verkauf unserer Vermögenswerte, gehören Ihre personenbezogenen Daten wahrscheinlich zu den übertragenen Vermögenswerten;

●      Bei entsprechenden rechtlichen Anforderungen (z.B. zur Unterstützung strafrechtlicher Ermittlungen oder anderer Rechtsverfahren); und/oder

●      Als Reaktion auf einen echten Notfall.

Außerdem kombinieren wir Ihre personenbezogenen Daten mit denen anderer Nutzer, um Trendinformationen weiterzugeben und Nutzerstatistiken mit Dritten zu verbinden, jedoch stets in zusammengefasster und anonymisierter Form.

Datenspeicherung: Die Speicherfrist für jedes durch Outbrain verwendete Cookie (gleich ob unser eigenes oder für uns durch Dritte) ist in der Cookie-Tabelle genannt:

<https://www.outbrain.com/legal/privacy#cookies>

Outbrain verfügt zudem über eine Richtlinie zur Datenspeicherung, in der die Speicherfrist für personenbezogene Daten aufgeführt ist, die auf unserer Analyse basiert, welche Speicherfrist für bestimmte Daten aus rechtlichen oder geschäftlichen Gründen angemessen ist. Wenn wir personenbezogene Daten nicht mehr benötigen, löschen oder vernichten wir diese auf sichere Weise. Zusammengefasste Daten, durch die kein Gerät/Browser (oder keine Person) identifiziert werden kann und die für die Berichterstattung und Analyse benötigt werden, behalten wir so lange, wie dies wirtschaftlich nötig ist.

In Übereinstimmung mit europäischen Datenschutzgesetzen, insbesondere der europäischen Datenschutz-Grundverordnung (DSGVO), gewährt Outbrain Bürgern der europäischen Gebiete bestimmte zusätzliche Rechte wie das Recht auf Zugriff, Berichtigung, Einspruch, Beschwerde, Löschung und Blockierung. Insbesondere:

das Recht auf Auskunft darüber, ob und welche personenbezogenen Daten von uns verarbeitet werden, sowie das Recht,

●      die Berichtigung oder Änderung personenbezogener Daten zu verlangen.

●      unter bestimmten Umständen das Recht, die Löschung personenbezogener Daten zu verlangen.

●      unter bestimmten Umständen das Recht, die Einschränkung der Verarbeitung personenbezogener Daten zu verlangen.

●      den jederzeitigen vollständigen oder teilweisen Widerruf Ihrer Zustimmung zur Verarbeitung und Nutzung Ihrer Daten mit zukünftiger Gültigkeit.

●      das Recht auf Erhalt Ihrer personenbezogenen Daten in einem üblichen, strukturierten und mechanisch lesbaren Format.

●      Kontaktaufnahme mit Ihrem Datenschutzbeauftragten bei Fragen, Anmerkungen, Beschwerden oder Anfragen im Zusammenhang mit unserer Datenschutzerklärung und der Verarbeitung Ihrer personenbezogenen Daten.

●      das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, falls Sie der Auffassung sind, dass die Verarbeitung Ihrer personenbezogenen Daten gesetzeswidrig ist.

Neben dem oben Genannten weist Outbrain in diesen Datenschutzbestimmungen auf bestimmte Rechte für Bürger des europäischen Gebiets hin. Laut der DSGVO bezeichnet die Formulierung "Bürger aus europäischen Gebieten" den Europäischen Wirtschaftsraum (EWR) und die Schweiz. Im Sinne dieser Datenschutzbestimmungen umfasst der Begriff "europäische Gebiete" weiterhin das Vereinigte Königreich, auch nachdem dieses den Europäischen Wirtschaftsraum im Anschluss an den Austritt (Brexit) verlässt. Bitte senden Sie eine Nachricht an [PrivacyQuestions@outbrain.com](mailto:PrivacyQuestions@outbrain.com), wenn Sie Fragen zur Ausübung dieser Rechte haben.

Wir setzen Outbrain nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#n-outbrain-ehemalig-ligatus)

**o.) emetriq**

Wir verwenden auf unserer Webseite "emetriq", einen Dienst der emetriq GmbH, Vorsetzen 35, 20459 Hamburg, Deutschland (nachfolgend bezeichnet als: "emetriq"). emetriq ermöglicht uns Nutzern, die unsere Webseite bereits einmal besucht und sich für unsere Angebote interessiert haben, auf dieser Webseite und auf Internetseiten, die ebenfalls emetriq verwenden, zielgerichtete Werbeanzeigen zu schalten. Die Einblendung dieser Werbung erfolgt auf Basis der Informationen, die emetriq bei einem Besuch des jeweiligen Nutzers auf der jeweiligen Webseite sammelt. emetriq verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unserer Webseite durch Sie ermöglichen. Dabei werden keine personenbezogenen Daten verarbeitet. In keinem Fall werden die vorgeschriebenen Informationen dazu verwendet, Sie als Besucher unserer Webseite persönlich zu identifizieren.

Wir verwenden emetriq zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unserer Webseite analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Die Verwendung von emetriq ermöglicht uns zudem, auf Ihre Interessen ausgelegte Werbung anzuzeigen.

Wir setzen emetriq nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unserer Webseite vollumfänglich nutzen können. Sie können die Erfassung der der vorgenannten Informationen durch emetriq auch dadurch verhindern, indem Sie auf einer der nachfolgend verlinkten Webseiten ein Opt-Out-Cookie setzen: <http://www.emetriq.com/opt-out/> oder <http://www.youronlinechoices.com/de/praferenzmanagement/>. Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen.

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite von emetriq entnehmen: <https://www.emetriq.com/datenschutz/>.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#o-emetriq)

**p.) Moat**

Wir verwenden auf unserem Internetauftritt "Moat", einen Dienst der Moat Inc., 228 Park Ave South #17953, New York NY 10003, USA (nachfolgend bezeichnet als: "Moat"). Moat speichert und verarbeitet Informationen über Ihr Nutzerverhalten auf unserem Internetauftritt. Moat verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unseres Internetauftritts durch Sie ermöglichen.

Wir verwenden Moat zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unseres Internetauftritts analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten.

Wir setzen Moat nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Sie können die Erfassung der vorgenannten Informationen durch Moat auch dadurch verhindern, indem Sie auf der nachfolgend verlinkten Webseite ein Opt-Out-Cookie setzen:

● <https://moat.com/privacy>

Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen. Sie können der Erfassung und Weiterleitung personenbezogenen Daten widersprechen oder die Verarbeitung dieser Daten verhindern, indem sie die Ausführung von Java-Script in Ihrem Browser deaktivieren. Zudem können Sie die Ausführung von Java-Script Code insgesamt dadurch verhindern, indem Sie einen Java-Script-Blocker installieren (z.B. <https://noscript.net/> oder [https://www.ghostery.com](https://www.ghostery.com/)). Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unseres Internetauftritts vollumfänglich nutzen können.

Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite entnehmen: <https://moat.com/privacy>

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#p-moat)

**q.) Yieldlab**

Wir verwenden auf unserer Webseite "Yieldlab", einen Dienst der Yieldlab AG, Colonnaden 41, 20354 Hamburg, Deutschland (nachfolgend bezeichnet als: "Yieldlab"). Yieldlab ermöglicht uns Nutzern, die unsere Webseite bereits einmal besucht und sich für unsere Angebote interessiert haben, auf dieser Webseite und auf Internetseiten, die ebenfalls Yieldlab verwenden, zielgerichtete Werbeanzeigen zu schalten. Die Einblendung dieser Werbung erfolgt auf Basis der Informationen, die Yieldlab bei einem Besuch des jeweiligen Nutzers auf der jeweiligen Webseite sammelt. Yieldlab verwendet hierfür unter anderem Cookies, also kleine Textdateien, die lokal im Zwischenspeicher Ihres Webbrowsers auf Ihrem Endgerät gespeichert werden und die eine Analyse der Benutzung unserer Webseite durch Sie ermöglichen. Yieldlab analysiert diese Cookies im Rahmen anschließender Besuche einzelner Webseiten, um hieraus gezielte Produktempfehlungen abzuleiten. Dabei werden keine personenbezogenen Daten verarbeitet. Diese Informationen werden nicht dazu verwendet, Sie als Besucher unserer Webseite persönlich zu identifizieren.

Wir verwenden Yieldlab zu Marketing- und Optimierungszwecken, insbesondere um die Nutzung unserer Webseite analysieren und um einzelne Funktionen und Angebote sowie das Nutzungserlebnis fortlaufend verbessern zu können. Durch die statistische Auswertung des Nutzerverhaltens können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Die Verwendung von Yieldlab ermöglicht uns zudem, auf Ihre Interessen ausgelegte Werbung anzuzeigen.

Wir setzen Yieldlab nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

Die Installation von Cookies können Sie verhindern, indem Sie vorhandene Cookies löschen und eine Speicherung von Cookies in den Einstellungen Ihres Webbrowsers deaktivieren. Wir weisen darauf hin, dass Sie in diesem Fall möglicherweise nicht alle Funktionen unserer Webseite vollumfänglich nutzen können. Sie können die Erfassung der der vorgenannten Informationen durch Yieldlab auch dadurch verhindern, indem Sie auf der nachfolgend verlinkten Webseite ein Opt-Out-Cookie setzen: <http://www.yieldlab.de/elements/privacy/>. Wir weisen Sie darauf hin, dass diese Einstellung gelöscht wird, wenn Sie Ihre Cookies löschen.

Weitere Informationen des Drittanbieters zum Datenschutz können Sie der nachfolgenden Webseite von Yieldlab entnehmen: <http://www.yieldlab.de/elements/privacy/>.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#q-yieldlab)

**r.) MaxMind**

Um Ihnen spezielle Services (z.B. automatische Vorauswahl Ihres Marktes) anbieten zu können, verwendet diese Webseite die von **MaxMind** (14 Spring Street, 3rd Floor

Waltham, MA 02451, USA) entwickelte Software zur **Geolokalisierung**. Diese Software analysiert Ihre IP-Adresse, um Ihren ungefähren Standort zu ermitteln. Die Geolokalisierung erfolgt ausschließlich auf Basis anonymisierter IP-Adressen. Eine genaue Standortermittlung des Webseitenbesuchers ist hierdurch ausgeschlossen.

Die Datenverarbeitung beruht auf unserem sich aus den Verarbeitungszwecken ergebenden unternehmerischen Interessen und beruht auf Art. 6 Abs. 1 lit. f) DSGVO. Wenn Sie MaxMind nicht nutzen wollen finden Sie nähere Informationen zur Deaktivierung unter:

<https://support.maxmind.com/de/maxmind-gdpr-faqs/information-about-the-general-data-protection-regulation-gdpr/how-does-maxmind-handle-data-subject-requests-to-exercise-their-rights-under-the-gdpr/>

Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#r-maxmind)

**s.) Tealium**

Im Bereich http://www.zeit.immowelt.de/ verwenden wir Tealium AudienceStream über welchen Daten erhoben und gespeichert werden, aus denen unter Verwendung von Pseudonymen Nutzungsprofile erstellt werden können. Zusätzlich wird das Tag-Management-System Tealium iQ eingesetzt, mit dem Messpixel von Drittanbietern auf unseren Seiten geladen werden. Zur Optimierung des Ladens der Messpixel erfasst Tealium über ein Cookie pseudonyme Daten. Wir werden diese Informationen benutzen, um Ihre Nutzung der Website automatisiert und in Echtzeit bedarfsgerecht zu gestalten.

Hierfür werden beispielsweise folgende Informationen erhoben:  
gesehene und geklickte Anzeigen, Artikel, Werbung, Besucherzahlen, Thema der Seite etc..  
Die pseudonymisierten Nutzungsprofile werden nur mit einer gesondert zu erteilenden und jederzeit widerruflichen Einwilligung  mit personenbezogenen Daten über den Träger des Pseudonyms zusammengeführt. Dies gilt auch für die Zusammenführung der von Ihrem Browser übermittelten IP-Adresse mit den Nutzungsprofilen. Die Rechtsgrundlage dieser Datenverarbeitung ist damit Art. 6 lit. a) DSGVO.      
Zur Erstellung der Nutzungsprofile werden Cookies oder bei mobilen Endgeräten ähnliche Technologien eingesetzt. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website werden ausschließlich in Deutschland gespeichert. Sie können die Speicherung der Cookies durch eine entsprechende Einstellung Ihrer Browser-Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website vollumfänglich werden nutzen können.

Sie können die Datenerhebung im Bereich <https://zeit.immowelt.de/> auch verhindern, indem Sie auf folgenden [Link](https://l3.evidon.com/site/5335/1772/3) klicken. Dabei wird ein Opt-Out-Cookie auf Ihrem Gerät gesetzt, der die zukünftige Erfassung Ihrer Daten beim Besuch dieser Webseiten verhindert. Löschen Sie Ihre Cookies, muss dieser Link erneut geklickt werden.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#s-tealium)

**t.) Twitter**

Auf unseren Seiten sind Funktionen des Dienstes Twitter eingebunden. Diese Funktionen werden angeboten durch die Twitter Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA. Durch das Benutzen von Twitter und der Funktion "Re-Tweet" werden die von Ihnen besuchten Webseiten mit Ihrem Twitter-Account verknüpft und anderen Nutzern bekannt gegeben. Dabei werden auch Daten an Twitter übertragen. Wir weisen darauf hin, dass wir als Anbieter der Seiten keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch Twitter erhalten. Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von Twitter unter <https://twitter.com/privacy>.

"Es ist nicht ausgeschlossen, dass Twitter Ihre Daten auch an die Muttergesellschaft, die Twitter Inc. mit Sitz in den USA, weiterleitet. Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender).

Ihre Datenschutzeinstellungen bei Twitter können Sie in den Konto-Einstellungen unter: <http://twitter.com/account/settings> ändern.

Twitter ist im "erweiterten Datenschutz-Modus" eingebunden, d.h. dass keine Daten über Sie als Nutzer an Twitter übertragen werden, wenn Sie die Twitter nicht zulassen. Erst wenn Sie der Einbindung zustimmen, werden Daten an den Twitter-Server übermittelt.

Wir setzen Twitter nur mit Ihrer Einwilligung ein, die sie jederzeit widerrufen können. Die entsprechende Datenverarbeitung beruht auf Art. 6 Abs. 1 lit. a) DSGVO. Die Speicherdauer beträgt 6 Monate.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#t-twitter)

**u.) Typeform**

"Für die Erhebung der Daten von Umfragen nutzen wir den Dienst "Typeform". Dieser Dienst wird von der TYPEFORM S.L., Carrer Bac de Roda, 163, 08018 Barcelona ("Typeform") zur Verfügung gestellt. Typeform gibt an, dass Ihre Antworten auf die im Rahmen der Umfrage gestellten Fragen, von Typeform nur dann eingesehen werden, wenn eine Fehlerbehebung stattfinden muss. Typeform verwendet nach eigenen Angaben Cookies, jedoch nur solche, welche keine personenbezogenen Daten erheben. Die Cookie-Einstellungen können in den Browser-Einstellungen bearbeitet werden. Typeform hat strenge Datenschutzrichtlinien, wickelt die Umfrageservices aber teilweise über den Cloud-Anbieter Amazon Web Services, Inc. ("AWS") mit Servern außerhalb der EU, mit Sitz in den USA, ab.  Weitere Details zur Datenübermittlung in Drittländer finden Sie im [TEIL I: Allgemeines](https://www.zeit.de/hilfe/datenschutz#d-datenuebermittlung-in-drittlaender)[.](https://www.zeit.de/hilfe/datenschutz#teil-i-allgemeines)

Nähere Informationen über die Verarbeitung Ihrer Daten durch Typeform können Sie den Datenschutzhinweisen von Typeform entnehmen: <https://admin.typeform.com/to/dwk6gt>.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#u-typeform)

**v.) Linkpulse**

Wir verwenden das Analysetool Linkpulse. Ein Unternehmen mit Sitz in Norwegen:  
Linkpulse AS, 981 500 334 (MVA), Idrettsveien 4, 1400 SKI, NORWAY.  
Persönliche Informationen, die Sie eindeutig identifizieren könnten, werden zu keinem Zeitpunkt erfasst. Linkpulse verwendet Cookies die eine Wiedererkennung eines Nutzers möglich machen, jedoch werden über diese Cookies keine personenbezogenen Daten gespeichert oder erfasst. Linkpulse gibt keine der erfassten Daten an Dritte weiter.

Die Verwendung von Linkpulse erfolgt mit berechtigtem Interesse nach Art. 6 Abs. 1 lit. f) DSGVO.

Detaillierte Informationen zum Datenschutz bei Linkpulse finden Sie – in englischer Sprache – auf der Seite <https://www.linkpulse.com/privacy>

Die Deaktivierung von LinkPulse cookies (opt-out) ist auf dieser Seite zu finden: <https://l3.evidon.com/site/5335/1772/3>

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#v-linkpulse)

**TEIL IV: Ihre Rechte**

Ihnen steht das Recht zu, jederzeit Auskunft über die bei uns gespeicherten personenbezogenen Daten einzuholen. Weiterhin haben Sie auch ein Recht auf Übertragbarkeit, Berichtigung oder Löschung sowie auf Einschränkung der Verarbeitung Ihrer Daten. Weiter können Sie jederzeit Widerspruch gegen die Verarbeitung Ihrer Daten erheben. Hierzu im Einzelnen:

**Verarbeitung bei der Ausübung Ihrer Rechte gem. Art. 15 bis 22 DSGVO**

Wenn Sie Ihre Rechte gemäß den Art. 12 bis 22 DSGVO ausüben, verarbeiten wir die übermittelten personenbezogenen Daten zum Zweck der Umsetzung dieser Rechte durch uns und um den Nachweis hierüber erbringen zu können. Zum Zweck der Auskunftserteilung und deren Vorbereitung gespeicherte Daten werden wir nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeiten und im Übrigen die Verarbeitung nach Maßgabe des Art 18 DSGVO einschränken. Diese Verarbeitungen beruhen auf der Rechtsgrundlage des Art. 6 Abs. 1 Buchst. c) DSGVO i.V.m. Art. 15 bis 22 DSGVO und § 34 Abs. 2 BDSG.  
Die Bearbeitung von Anträgen nach Art. 15 bis 22 DSGVO erfolgt für die ZEIT-Verlagsgruppe durch den Zeitverlag Gerd Bucerius GmbH & Co. KG, Buceriusstraße, Eingang Speersort 1, 20095 Hamburg. Die Übermittlung beruht auf der Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f) DSGVO und dient unserem Interesse, Verarbeitungen in der Unternehmensgruppe effizient zu organisieren.

Sofern Datenverarbeitungen in gemeinsamer Verantwortlichkeit erfolgen, können Sie Ihre Betroffenenrechte bei der Zeitverlag Gerd Bucerius GmbH & Co. KG und jedem weiteren Verantwortlichen geltend machen.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#teil-iv-ihre-rechte)

**a.) Recht auf Auskunft**

Sie haben nach Art. 15 DSGVO ein Recht dazu, von uns eine Bestätigung darüber zu verlangen, ob Sie betreffende personenbezogene Daten verarbeitet werden. Sofern dies der Fall ist, haben Sie weiter ein Recht auf Auskunft über diese personenbezogenen Daten und auf Informationen zum Verarbeitungszweck, der Kategorie personenbezogener Daten, die verarbeitet werden, die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, die geplante Dauer für die, die personenbezogenen Daten gespeichert werden, das Bestehen eines Rechtes auf Berichtigung oder Löschung der Sie betreffenden Daten oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechtes gegen diese Verarbeitung, das Bestehen eines Beschwerderechtes bei einer Aufsichtsbehörde sowie, wenn die personenbezogenen Daten nicht bei Ihnen selbst erhoben wurden, auf alle verfügbaren Informationen über die Herkunft der Daten.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#a-recht-auf-auskunft)

**b.) Recht auf Berichtigung**

Nach Art. 16 DSGVO haben Sie weiter das Recht unverzüglich die Berichtigung oder Vervollständigung Sie betreffender unrichtiger personenbezogener Daten zu verlangen.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#b-recht-auf-berichtigung)

**c.) Recht auf Löschung**

Unter den in Art. 17 DSGVO genannten Voraussetzungen haben Sie das Recht die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#c-recht-auf-loeschung)

**d.) Recht auf Einschränkung**

Unter den Voraussetzungen des Art. 18 DSGVO haben Sie das Recht die Einschränkung der Verarbeitung Ihrer Daten zu verlangen.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#d-recht-auf-einschraenkung)

**e.) Recht auf Übermittlung**

Nach Art. 20 DSGVO haben Sie das Recht, die Sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, sowie das Recht, sofern die Voraussetzungen des Art. 20 DSGVO vorliegen, diese einem anderen Verantwortlichen zu übermitteln. In diesem Zusammenhang haben Sie das Recht, dass die Sie betreffenden personenbezogenen Daten direkt an die anderen Verantwortlichen übermittelt werden.

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#e-recht-auf-uebermittlung)

**f.) Recht auf Widerspruch**

**Nach Art. 21 DSGVO haben Sie, sofern Ihre personenbezogenen Daten auf Grundlage von berechtigten Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO verarbeitet werden, das Recht, gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten einzulegen, soweit dafür Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben.**

**Gegen die Verarbeitung Ihrer Daten zum Zwecke der Direktwerbung haben Sie das Recht, dieser Verarbeitung ohne Angabe einer besonderen Situation jederzeit zu widersprechen.**

**Möchten Sie von Ihrem Widerrufs- oder Widerspruchsrecht Gebrauch machen, genügt eine E-Mail an**[**email@zeit.de**](mailto:diezeit@zeit.de)**.**

[LINK KOPIEREN](https://www.zeit.de/hilfe/datenschutz#f-recht-auf-widerspruch)

**g.) Recht auf Beschwerde bei der Aufsichtsbehörde**

Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der zuständigen Aufsichtsbehörde beschweren.

**Sie erreichen uns unter folgenden Kontaktdaten**:

Zeit Online GmbH

Buceriusstraße, Eingang Speersort 1  
20095 Hamburg

Telefon: 040 / 32 80-0  
Fax: 040 / 32 71 11  
E-Mail: [email@zeit.de](mailto:email@zeit.de?subject=Datenschutzanfrage)

Veracrypt

Privacy Policy

Effective Date: October 2, 2011

As we develop software whose purpose is to ensure and protect privacy, it is needless to say that we recognize that privacy is very important. We respect your privacy. This Privacy Policy applies to the official VeraCrypt website ("this website"), which is located at www.veracrypt.fr.

No personally identifiable information of internet users visiting this website is collected by/on this website.\* However, note that it is sometimes possible, under certain circumstances, to determine with a high degree of accuracy who used a certain Internet Protocol address at a particular time (we are not able to do so, but, for example, law enforcement agencies are able and entitled to do so in some cases). Consequently, an Internet Protocol address may be considered potentially personally identifiable information in some cases. When you visit this website, your internet browser (e.g. Internet Explorer or Firefox) sends and receives data to/from the server software, Apache. The server software automatically records some of the information that your internet browser sends to it or that the server software otherwise obtains automatically in connection with your web request. For instance, it records the type of your browser, browser language, type of operating system, referring website, Internet Protocol address, and the date and time of your request. We use some of the information to analyze attacks on our server (and abuse of our website) and to help ensure that they are not successful. We also use some of the information when developing or testing VeraCrypt (e.g., we determine the percentage of users who use a particular version of an operating system). Furthermore, we use some of the information to evaluate the success of the VeraCrypt project in various countries (e.g. by determining the average number of visitors from a particular country per day) and when optimizing or testing our website (e.g., we determine the most used types of browsers, which we then use to test our website and for which we optimize it). All the information is encrypted so that it is very difficult for unauthorized persons to access it. We will not disclose the information to any third party without your consent, unless we need to do so in order to prevent (or to facilitate analysis of) attacks on our server, or abuse of this website, and/or unless we are required to do so by law.

This website reads and writes cookies containing solely anonymous traffic data, which we use to evaluate the success of the VeraCrypt project (e.g. by determining the average number of returning visitors per day and the average frequency of repeated visits per visitor). Cookies are small text files that your internet browser stores locally for websites you visit. You can prevent cookies from being stored/sent/received by configuring your internet browser (for example, in Internet Explorer, select Tools > Internet Options > Privacy, or in Firefox, select Tools > Options > Privacy).

We reserve the right to change this Privacy Policy from time to time. However, if we do, most changes will be minor. Each version of this Privacy Policy is identified at the top of this page by its effective date.

Wickr Messenger

**Wickr Messenger (Wickr Me App)**

**Our Privacy Practices in Brief:**  
Wickr has to collect some information from you in order to provide our Services to you, but we do so in a highly limited, highly secure way.

* We can’t see information you send through the Wickr Me App. Your information is always disguised with multiple rounds of salted, cryptographic hashing before it is transmitted to our servers. Because of this we don’t know — and can’t reveal to others — anything about you or how you use the Wickr Me App aside from the limited information such as the date your account was created, the date of last use and the type of device on which such account was installed. Please see our [Legal Process Guidelines](https://wickr.com/privacy/#legalprocess) for more details.
* Wickr does not log or store metadata associated with your use of the Wickr Me App.
* When you send end-to-end encrypted ephemeral files using Wickr Me, it is important to note that if you do not trust the person you’re talking to, do not open files coming from them or send them photos/files you do not want to be saved.
* You control how long your messages are accessible to the recipients, through expiration, burn-on-read settings, and the recall feature which allows you to retract a message you sent. However, there is no magic pill for betrayal and we cannot prevent someone using a camera to take a picture of a message on a screen. Therefore, we strongly encourage you to only send private messages or sensitive information to people you know and trust.
* When you block someone from being able to contact you on Wickr Me, they are automatically added to the block list in your settings. To protect your privacy, they won’t know that you are blocking them when they send you a message.
* If you enabled message notifications for Wickr Me, you will receive notifications about incoming messages on your device’s home screen which will contain the sender’s name as you set it in your Wickr contacts. You can also enable message preview in Wickr settings for notifications, which will add the content of a message to the home screen notifications. Please note, if you don’t want other to see who is messaging you on Wickr Me, you can disable notifications in your device settings in which case you will continue to receive messages, but notifications will not appear on your home screen.
* You own your data. We do not share or sell any data about our users. Period.

**What Information Does Wickr Collect and How Is It Used?**  
We are committed to limiting our collection of your information to what is necessary to provide you with our Services in accordance with applicable data protection and privacy laws.

The limited information we collect, receive, or have access to is used to provide the Service, to allow you to send and receive messages and files, to respond to your requests, and to improve the Service, in line with the legitimate interest we have in delivering the Services to you. It may also be shared under valid legal process and with third party service providers for the limited purposes described below.

**What We Don’t Collect**  
Equally important to us is to share what information we don’t collect. We do not collect your location information or have access to the contents of the communications you send using the Wickr Me App. Remember, however, that if you send a Wickr message to another Wickr user, that message or related content might remain on their device even after you delete it from yours, depending on the value you set for the expiration or burn-on-read time of that message and whether the recipient took a screenshot of the message.

**User-Provided Information**  
We collect some very limited information from you after you download the Wickr Me App in order to allow you to create a Wickr Me Account, and begin using the Wickr Me App.

* **Your Wickr ID:** Your Wickr ID is how you allow others to contact you via Wickr Me. It does not have to be your real name or provide any reference to your identity. Like other information pertaining to your account, it is disguised with multiple rounds of salted, cryptographic hashing when we associate it with your Device Information (described below). The purpose of this cryptographic representation is to allow you to use our Services without our needing to know who you are.
* **Your Password:** We require you to have a password to use the Wickr Me App, but we never store your password on our servers and don’t store it by default in any form on your device. For your own security, we recommend that you use a long, unique password consisting of a mix of upper- and lower-case letters, numbers, and symbols.

**Optional User-Provided Information**  
Within the Wickr Me App, we provide a few optional features for your convenience. Some of these features, described below, will ask for personal information. If you want to keep your use of Wickr Me as anonymous as possible, please read these sections carefully in order to understand how we associate information you provide with your Wickr Me account.

* **Push Notifications:** When setting up your Wickr Me account, we will ask if you want to receive notifications of new Wickr messages, software updates, and other administrative and technological developments. Push notifications are functions of devices operating system, so if you enable this feature, your devices operating system’s manufacturer will know that you are using the Wickr Me App, but will not know anything about how you use it or be able to see anything you transmit through it.
* **ID Connection:** To allow your friends to find you on Wickr Me without knowing your Wickr ID, you may choose to associate your other contact information — currently, just your phone number— with your Wickr ID. When you use this feature, we disguise your contact information with multiple rounds of salted cryptographic hashing for storage on our servers. This way, you can let your friends search for you on Wickr Me without revealing your contact information to us. If you use ID Connect to associate your phone number with your Wickr ID, we use a third party service Twilio solely to deliver a confirmation SMS to you, but that party will not receive any information about you other than your phone number, and the SMS message itself will contain no information except a confirmation link.
* **Invitations:** If you wish to invite others to use the Wickr Me App, you will be asked for permission to access your device’s contacts in order to invite them to use our Services. We never store your device contacts on our servers in any way. All invitations are generated locally on your device, without sharing any information with us.
* **Contact Finder:** Contact Finder allows you to search for contacts who have used ID Connect to associate their phone number with their Wickr accounts. If you use Contact Finder, the Wickr Me App will send a disguised representation of your contacts’ phone numbers to our servers to ensure that our server never accesses your actual contact list. We never store your device contacts in any form on our servers.
* **Encrypting Cloud Data:** The Wickr Me App will allow you to share files you have stored with cloud storage services Google Drive, Dropbox, and Box. The Wickr Me App will make encrypted copies of such files when sending as Wickr messages, which expire when the message self-destructs or is recalled. Cloud storage of your files on Google Drive, Dropbox and Box will be governed by these cloud storage services’ terms, conditions, and privacy policies, so please familiarize yourself with those documents before you use this feature.
* **Key Verification:** To validate the identities of your contacts, the Wickr Me App offers a video key verification mechanism. You can send a validation request to one of your Wickr contacts when establishing connections. You will then be asked to record a short ID verification video, which will be used to validate your identity with your contacts. If the ID video verification you receive from any of your contacts does not appear authentic, you can decline to verify their identity, thus rejecting the connection. Your verification video is encrypted before it is transmitted to our servers, which renders it inaccessible to Wickr. If you decide to re-record your ID verification video, your previous video is automatically deleted from our servers. You can learn more about video key verification [here](https://medium.com/cryptoblog/key-verification-in-secure-messaging-bd93a1bf3d40).
* **Avatar:**You can set a public profile avatar, which will become visible to others on Wickr Me so please do not add an avatar if you do not intend it to be viewed by others users.

**Automatically Collected Information**  
Wickr collects two types of information automatically during your setup and use of the Wickr Me App: Device Information, Aggregate Usage Data, and Crash Logs.

* **Device Information:** The Wickr App may collect hashed representations of your mobile device’s hardware ID and/or other platform-related information during registration. This information is used to tie your account to your device.
* **Aggregate Usage Data:** During the operation of our services, we also collect aggregate, anonymous information about basic usage statistics, such as the number of messages sent by all Wickr Me users daily, what types of messages our users tend to send (e.g., voice messages more often than text), and so forth. We never attempt to (and cannot) identify users associated with any of this information.
* **Crash Logs:** For the purpose of debugging, error correction, and system continuity, Wickr Apps transmit crash logs to a cloud-based bug reporting platform. The logs do not contain any user personal information and they pertain only to the Wickr Me App.

**What Information Does Wickr Share with Third Parties?**  
We do not share any user information we have with third parties, with the exception of the third-party service with whom we share your phone number for the sole purpose of sending you an SMS confirmation if you choose to associate your phone number with your Wickr Me ID. Please note that the provision of a phone number is completely at the user’s discretion.

**Law Enforcement:**  
Please see our full [Legal Process Guidelines](https://wickr.com/privacy/#legalprocess), but here are the highlights:

We will always notify our users of any third party requests for their information unless we are legally prohibited from doing so. As soon as legally permissible, we will notify our users of requests for their information. We require a warrant before handing over the contents of communications; however, because of the nature of our technology, the contents of communications will be encrypted and undecipherable if obtained.

**You Can Terminate Your Account**  
You can terminate your account at any time. Once terminated, your account will be irrevocably suspended, ensuring that nobody can use that Wickr ID again in order to prevent impersonation. If you wish to terminate your Wickr Me account, go to Settings, “Terminate Account” and verify by entering your password.

**We Retain As Little Data As Possible, for the Least Time Possible**

**Data Retention on Wickrʼs Servers:**Our servers store the encrypted messages that you send and receive for up to 6 days to ensure their reliable delivery to each device associated with your account and the accounts to which you transmit messages. We retain certain account data (i.e., types of messages sent and account settings changes) which contain no PII for up to 6 days.

**Data Retention on Your Device:** All messages are stored in encrypted form on end users’ devices. You choose your own retention policy for your messages by choosing how long a message is viewable before it is deleted (via the expiration or burn-on-read time for sent messages, recall ability and manual deletion for your device). In addition, Wickr’s “[secure shredder](https://support.wickr.com/hc/en-us/articles/115004958407-What-does-the-Secure-Shredder-do-)” technology uses forensic deletion techniques to help reduce the risk of deleted messages and temporary data being recovered.

**We Are Serious About Security**  
We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees who need to know that information in order to operate, develop, or improve our Services. No sensitive information is in the clear: we take reasonable efforts (as described herein) to ensure that everything we store is not retrievable by us or anyone else.

However, as security experts, we know that no security system can prevent all potential security breaches. Therefore, we have limited the potential implications of such a breach by designing our system so that in the event of a breach, we would have the least possible information about you.

Wickr’s network infrastructure and services are maintained in highly secure, strategically located data centers managed by Amazon Web Services (AWS). Learn more about AWS security policies [here](https://aws.amazon.com/security/).

**Children**  
Wickr is not directed to children under the age of 13. If we learn that we have allowed a child under 13 to access our Services, we will take appropriate steps to promptly remove such account and delete all information associated with such account.

If you live in any other country except those in the European Region, you must be at least 13 years old to register for the Services. If you live in the European Region, you must be at least 16 years old to register for and use our Services.

**Customer Service**  
In an ongoing effort to improve our services and assist our customers with any questions they have about the use of the Wickr Me App, we have developed a comprehensive collection of the most commonly asked customer support questions and answers, which are available [here](https://support.wickr.com/). Any information provided to us by our users voluntarily when they request customer support (e.g., an email address, Wickr Me App version, or any other details related to user issue) will be used to respond to that individual request and may be logged as part of our effort to improve our customer service and solve any product-related issues. This user-provided information cannot be linked to our users Wickr Me accounts, unless users voluntarily include their Wickr Me account information in their customer service-related requests. We strongly discourage our users from disclosing their passwords to Wickr Me accounts to third parties.

**Cookie Policy**  
We tirelessly work on improving our services and raising awareness about our products, which are designed to ensure our users’ security and privacy. To accomplish these goals, we use cookies on the Wickr website that enable us to learn how visitors navigate our content and interact with our marketing materials so we can be more effective at informing our users about product developments.

A cookie is a small text file that is placed in visitors’ browsers to help us learn when users arrive at our site, how they use the site, when they leave, and when they come back. These cookies can never be used to identify user accounts within the Wickr App.

Here is an example of how we may use information collected via cookies: we may think that one of our new features would be very useful to the Wickr community, but cookies may tell us that very few users fully read that feature’s description on our site. That insight would help us to rethink the way we explain that product on our site or present it in an advertisement so that we can better communicate our services to our users.

We make every reasonable effort to minimize the information we collect. For example, we enforce IP masking for the website analytics purposes to conceal the last 4 digits of IP addresses which ensures that visitor’s full IP addresses are not collected via third party services such as Google Analytics.

We provide the utmost transparency on and an up-to-date overview of cookies used on our website including the ability for website visitors to [check, withdraw or modify](https://wickr.com/privacy/#cookiedeclaration) consent for non-necessary cookies at any time. More information on our Cookie Policy can be found [here](https://wickr.com/privacy/#cookies).

**Web Forms**  
To enable our visitors to reach out to us with sales inquiries, we may collect information using online form submissions. Please note that all information you provide via web forms on our site is strictly voluntary and will never be used in any way that is inconsistent with other provisions of this Privacy Policy.

**Third Parties**  
To improve Wickr’s products, website, or marketing, we may engage with various outside partners that have access to the limited data users voluntarily share with Wickr via web forms, cookies, or customer support and sales inquiries. We carefully select each of our partners based on Wickr’s commitment to user privacy and security. Our security team meticulously vets each prospective partner to ensure its policies and practices are on par with Wickr’s standards.

* To assist Wickr with improving our web content and advertising activities, we partner with [Pardot](http://www.pardot.com/), a B2B Marketing Automation Platform, and [Salesforce](https://salesforce.com/).
* To accelerate resolution of the most frequent customer inquiries, Wickr’s support is automated in collaboration with [Zendesk](https://zendesk.com/), a customer support platform.
* To deliver a confirmation SMS to our users opting in to connect with friends via ID Connect, we use [Twilio](https://twilio.com/).
* To host our website, we use [WP Engine](http://wpengine.com/).
* To maintain high-security, fast and reliable service delivery worldwide, Wickr partners with [AWS](https://aws.amazon.com/privacy/), a global infrastructure provider.
* To manage bug reports, we use [Bugsnag](https://www.bugsnag.com/), a cloud-based bug reporting platform.

Each of these companies has its own policies for handling user data. Please review the respective privacy policies for [Zendesk](http://www.zendesk.com/privacy), [Twilio](https://www.twilio.com/legal/privacy), [Pardot](http://www.pardot.com/company/legal/privacy-policy/), [WP Engine](https://www.wpengine.com/legal/privacy), [AWS](https://aws.amazon.com/privacy/), and [Bugsnag](https://docs.bugsnag.com/legal/privacy-policy/) for a more complete understanding of their practices.

If you have additional questions regarding our privacy protection practices, please email us at [privacy@wickr.com](mailto:privacy@wickr.com).

**We Can Change This Privacy Policy**  
This Privacy Policy may be updated from time to time, for any reason. We will notify you of any changes to our Privacy Policy by posting the new Privacy Policy here along with information about what has changed and an archive of past policies. You are advised to consult this Privacy Policy regularly for any changes. By continuing to use the Services, you agree to be bound by the revised Privacy Policy.

**Users Outside the US**  
If you use our Services, your information will be transferred to the U.S. and will be processed and stored under U.S. data protection and privacy regulations which may differ from those your country of residence. By using our Services and providing information to us, you consent to such transfer to and processing in the U.S. We take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this policy. Please note that all user communications on the Wickr Service are protected between devices and are never stored unencrypted hence are undecipherable to Wickr or other third parties.

You are responsible for complying with any laws or regulations in your country that govern use of applications and services like Wickr Me.

**Contact Us if You Have Questions or Account-Related Requests**  
If you have any questions regarding privacy while using our Services, or have questions about our practices, please contact us via email at [privacy@wickr.com](mailto:privacy@wickr.com).

If you live in the European Region, please note the following:

**Opt-out.**You may contact us anytime to opt-out of:

* direct marketing communications or
* the transfer of your personal data outside the European Region. Please note that your use of some of the Service may be affected by your opt-out.

**Access.** You may access the data we hold about you at any time within the application or by contacting us directly.

**Amend.** You can also contact us to update or correct any inaccuracies in your personal data.

**Erase and forget.** In certain situations, for example, when the data we hold about you is no longer relevant or is incorrect, you can request that we erase your data. Please note that only you can delete your Wickr Me account at any time form within the Service, due to privacy design of the Service, we are unable to delete Wickr Me accounts upon your request.

You may contact us at [gdpr@wickr.com](mailto:gdpr@wickr.com) on any questions you may have about your personal data and our use of such personal data under the GDPR.

Telegram

**Telegram Privacy Policy**

**1. Introduction**

This Privacy Policy sets out how we, Telegram Messenger Inc. **(“Telegram”)**, use and protect your personal data that you provide to us, or that is otherwise obtained or generated by us, in connection with your use of our cloud-based messaging services (the **“Services”**). For the purposes of this Privacy Policy, **‘we’**, **‘us’** and **‘our’** refers to Telegram, and **‘you’** refers to you, the user of the Services.

**1.1 Privacy Principles**

Telegram has two fundamental principles when it comes to collecting and processing private data:

* We don't use your data to show you ads.
* We only store the data that Telegram needs to function as a secure and feature-rich messaging service.

**1.2. Terms of Service**

This Privacy Policy forms part of our Terms of Service, which describes the terms under which you use our Services and which are available at [**https://telegram.org/tos**](https://telegram.org/tos). This Privacy Policy should therefore be read in conjunction with those terms.

**1.3. Table of Contents**

This Privacy Policy explains the following:

* [the legal basis for processing your personal data;](https://telegram.org/privacy#2-legal-ground-for-processing-your-personal-data)
* [what personal data we may collect from you;](https://telegram.org/privacy#3-what-personal-data-we-use)
* [how we keep your personal data safe;](https://telegram.org/privacy#4-keeping-your-personal-data-safe)
* [what we may use your personal data for;](https://telegram.org/privacy#5-processing-your-personal-data)
* [who your personal data may be shared with;](https://telegram.org/privacy#8-who-your-personal-data-may-be-shared-with) and
* [your rights regarding your personal data.](https://telegram.org/privacy#9-your-rights-regarding-the-personal-data-you-provide-to-us)

**1.4. EEA Representative**

If you live in a country in the [European Economic Area](https://en.wikipedia.org/wiki/European_Economic_Area) (EEA), the Services are provided by Telegram, which for the purposes of applicable data protection legislation is the data controller responsible for your personal data when you use our Services. However, as Telegram is located outside the EEA, we have designated one of our EEA-based group companies, Telegram UK Holdings Ltd (71-75 Shelton Street, Covent Garden, London, England, WC2H 9JQ), as a representative to whom you may direct any issues you have relating to our processing of your personal data.

**2. Legal Ground for Processing Your Personal Data**

We process your personal data on the ground that such processing is necessary to further our legitimate interests (including: *(1)* providing effective and innovative Services to our users; and *(2)* to detect, prevent or otherwise address fraud or security issues in respect of our provision of Services), unless those interests are overridden by your interest or fundamental rights and freedoms that require protections of personal data.

**3. What Personal Data We Use**

**3.1. Basic Account Data**

Telegram is a communication service. You provide your mobile number and basic account data (which may include profile name, profile picture and about information) to create a Telegram account.

To make it easier for your contacts and other people to reach you and recognize who you are, the screen name you choose, your profile pictures, and your [username](https://telegram.org/faq#usernames-and-t-me) (should you choose to set one) on Telegram are always public. We don't want to know your real name, gender, age or what you like.

We do **not** require your screen name to be your real name. Note that users who have you in their contacts will see you by the name they saved and not by your screen name. This way your mother can have the public name 'Johnny Depp' while appearing as 'Mom' to you and as 'Boss' to her underlings at work (or the other way around, depending on how these relationships are structured).

**3.2. Your E-mail Address**

When you enable 2-step-verification for your account or store documents using the Telegram Passport feature, you can opt to set up a password recovery email. This address will only be used to send you a password recovery code if you forget it. That's right: no marketing or “we miss you” bullshit.

**3.3. Your Messages**

**3.3.1. Cloud Chats**

Telegram is a cloud service. We store messages, photos, videos and documents from your *cloud chats* on our servers so that you can access your data from any of your devices anytime without having to rely on third-party backups. All data is stored heavily encrypted and the encryption keys in each case are stored in several other data centers in different jurisdictions. This way local engineers or physical intruders cannot get access to user data.

**3.3.2. Secret Chats**

*Secret chats* use end-to-end encryption. This means that all data is encrypted with a key that only you and the recipient know. There is **no way** for us or anybody else without direct access to your device to learn what content is being sent in those messages. We do not store your secret chats on our servers. We also do not keep any logs for messages in secret chats, so after a short period of time we no longer know who or when you messaged via secret chats. For the same reasons secret chats are not available in the cloud — you can only access those messages from the device they were sent *to* or *from*.

**3.3.3. Media in Secret Chats**

When you send photos, videos or files via secret chats, before being uploaded, each item is encrypted with a separate key, not known to the server. This key and the file’s location are then encrypted again, this time with the secret chat’s key — and sent to your recipient. They can then download and decipher the file. This means that the file is technically on one of Telegram’s servers, but it looks like a piece of random indecipherable garbage to everyone except for you and the recipient. We don’t know what this random data stands for and we have no idea which particular chat it belongs to. We periodically purge this random data from our servers to save disk space.

**3.3.4. Public Chats**

In addition to private messages, Telegram also supports public channels and public groups. All public chats are cloud chats (see [section 3.3.1 above](https://telegram.org/privacy#3-3-1-cloud-chats)). Like everything on Telegram, the data you post in public communities is encrypted, both in storage and in transit — but everything you post in public will be accessible to everyone.

**3.3.5. Phone Number and Contacts**

Telegram uses phone numbers as unique identifiers so that it is easy for you to switch from SMS and other messaging apps and retain your social graph. We ask your permission before syncing your contacts.

We store your up-to-date contacts in order to notify you as soon as one of your contacts signs up for Telegram and to properly display names in notifications. We only need the number and name (first and last) for this to work and store no other data about your contacts.

Our automatic algorithms can also use anonymized sets of phone numbers to calculate the average number of potential contacts an unregistered phone number may have on Telegram. When you open the 'Invite friends' interface, we display the resulting statistics next to your contacts to give you an idea of who could benefit most from joining Telegram.

You can always stop syncing contacts or delete them from our servers in Settings > Privacy & Security > Data Settings.

If you are using Android, Telegram will ask you for permission to access your phone call logs (READ\_CALL\_LOG). If you grant this permission, Telegram will be able verify your account by transmitting a phone call instead of asking you to enter a code. Telegram uses this permission only to confirm receipt of the confirmation call by verifying the number in the call log.

**3.3.6. Cookies**

The only cookies we use are those to operate and provide our Services on the web. We do not use cookies for profiling or advertising. The cookies we use are small text files that allow us to provide and customize our Services, and in doing so provide you with an enhanced user experience. Your browser should allow you to control these cookies, including whether or not to accept them and how to remove them. You may choose to block cookies with your web browser, however, if you do disable these cookies you will not be able to log in to Telegram Web.

**4. Keeping Your Personal Data Safe**

**4.1. Storing Data**

If you signed up for Telegram from the UK or the EEA, your data is stored in data centers in the Netherlands. These are third-party provided data centers in which Telegram rents a designated space. However, the servers and networks that sit inside these data centers and on which your personal data is stored are owned by Telegram. As such, we do not share your personal data with such data centers. All data is stored heavily encrypted so that local Telegram engineers or physical intruders cannot get access.

**4.2. End-to-End Encrypted Data**

Your messages, media and files from secret chats (see [section 3.3.2](https://telegram.org/privacy#3-3-2-secret-chats) above), as well as the contents of your calls and the data you store in your [Telegram Passport](https://telegram.org/blog/passport) are processed only on your device and on the device of your recipient. Before this data reaches our servers, it is encrypted with a key known only to you and the recipient. While Telegram servers will handle this end-to-end encrypted data to deliver it to the recipient – or store it in the case of Telegram Passport data, we have no ways of deciphering the actual information. In this case, we neither store nor process your personal data, rather we store and process random sequences of symbols that have no meaning without the keys which we don’t have.

**4.3. Retention**

Unless stated otherwise in this Privacy Policy, the personal data that you provide us will only be stored for as long as it is necessary for us to fulfill our obligations in respect of the provision of the Services.

**5. Processing Your Personal Data**

**5.1. Our Services**

Telegram is a cloud service. We will process your data to deliver your cloud chat history, including messages, media and files, to any devices of your choosing without a need for you to use third-party backups or cloud storage.

**5.2. Safety and Security**

Telegram supports massive communities which we have to police against abuse and Terms of Service violations. Telegram also has more than [400 million](https://telegram.org/blog/400-million) users which makes it a lucrative target for spammers. To improve the security of your account, as well as to prevent [spam](https://telegram.org/faq_spam), abuse, and other violations of our Terms of Service, we may collect metadata such as your IP address, devices and Telegram apps you've used, history of username changes, etc. If collected, this metadata can be kept for 12 months maximum.

**5.3. Spam and Abuse**

To prevent phishing, spam and other kinds of abuse and violations of Telegram’s Terms of Service, our moderators may check messages that were reported to them by their recipients. If a spam report on a message you sent is confirmed by our moderators, your account may be limited from contacting strangers – temporarily or permanently. You can send an appeal using [@Spambot](https://t.me/spambot). In case of more serious violations, your account may be banned. We may also use automated algorithms to analyze messages in cloud chats to stop spam and phishing.

**5.4. Cross-Device Functionality**

We may also store some aggregated metadata to create Telegram features (see [section 5.5](https://telegram.org/privacy#5-5-advanced-features) below) that work across all your devices.

**5.5. Advanced features**

We may use some aggregated data about how you use Telegram to build useful features. For example, when you open the Search menu, Telegram displays the people you are more likely to message in a box at the top of the screen. To do this, we calculate a rating that shows which people you message frequently. A similar rating is calculated for inline bots so that the app can suggest the bots you are most likely to use in the attachment menu (or when you start a new message with “@”). To turn this feature off and delete the relevant data, go to Settings > Privacy & Security > Data Settings and disable “Suggest Frequent Contacts”.

**5.6. No Ads**

Unlike other services, we don't use your data for ad targeting or other commercial purposes. Telegram only stores the information it needs to function as a secure and feature-rich cloud service.

**6. Bot Messages**

**6.1. Ecosystem**

Telegram has an API that allows third-party developers to create [bots](https://core.telegram.org/bots). Bots are apps that look like special Telegram users: you can talk to them from your chat list, add them to groups or use a special [“inline”](https://telegram.org/blog/inline-bots) interface to access their features. By performing any of these actions, you will be sending some of your data to the respective third-party bot developers.

**6.2. How Bots Can Receive Data**

You can send data to bot developers when you interact with their bots in one of these ways:

* By sending messages to a bot.
* By using an [inline bot](https://telegram.org/blog/inline-bots).
* By participating in a group with a bot.
* By pressing buttons in messages sent by a bot.
* By paying for goods and services via bots (see [section 7](https://telegram.org/privacy#7-third-party-payment-services) below).

**6.3. What Data Bots Receive**

In any of the above cases, the developers of an automated user (bot) can get your public account data (see [section 3.1](https://telegram.org/privacy#3-1-basic-account-data) above): your screen name, username and profile picture(s).

Bots can also receive the following data when you **interact** with them.

* Bots will obviously get your messages when you send them something.
* If you click on links or buttons provided by the bot, the bot can potentially get your IP address (provided that it controls the website to which the link leads).
* If the bot is a member of the same group with you, it may know you are a member.
* When you start your message with the username of an [inline bot](https://telegram.org/blog/inline-bots) (e.g. [@gif](https://t.me/gif)) the interface transforms so that everything you type becomes a query to that bot. This query is sent to the bot so that it can provide its service. We will warn you about this the first time you use an inline bot.
* Bots added to groups can operate in two modes: with access to messages in the group or [without access](https://core.telegram.org/bots#privacy-mode). If the bot has access to messages, it can see everything that happens in the group. The interface clearly shows whether or not a bot has access to messages in groups.

**6.4. Bots Are Not Maintained by Telegram**

Other than our own bots, no other bots or third-party bot developers are affiliated with Telegram. They are completely independent from us. They should ask you for your permission before they access your data or you make it available to them.

**7. Third Party Payment Services**

**7.1. Payment Information**

The [Payment Platform for Bots](https://core.telegram.org/bots/payments) is available to users as of [Telegram 4.0](https://telegram.org/blog/payments). Telegram does not process payments from users and instead relies on different payment providers around the world. It is the payment providers that handle and store your credit card details. Neither Telegram nor the merchants on the platform (bot developers) have access to this information. Although we work with payment providers they are completely independent from Telegram. Please study their relevant privacy policies before making your data available to them.

**7.2. Credit Card Information**

When making a purchase, you enter your credit card details into a form supplied by the payment provider that will be processing the payment, and this information goes directly to the payment provider's server. Your credit card information never reaches Telegram's servers. We do not access and do not store your credit card information. When you save your credit card info, it is saved on the respective payment provider's servers and the payment provider gives Telegram a *token* that you can reuse for future payments. It is not possible to reconstruct your credit card info from the token.

**7.3 Shipping Information**

When you enter shipping information in the process of placing an order, we send it directly to the merchant bot developer. We can store your shipping information for you if you choose to save it for future purchases. We will delete this information immediately if you ask us to.

**7.4. Clearing Payment Information**

You can clear all payment information associated with your account at any time by going to Telegram Settings > Privacy & Security > Data Settings and selecting ‘Clear Payment & Shipping Info’. If you choose to remove your payment information, we will delete your stored shipping info and payment tokens from all providers and ask the payment providers to remove your credit card information that they store.

**7.5. Payment Disputes**

Due to the fact that Telegram doesn't store any credit card details or transaction information, it is impossible for us to handle complaints or cashbacks – any disputed payments are the responsibility of the bot developers, payment providers, and banks that participated in the exchange.

**8. Who Your Personal Data May Be Shared With**

**8.1. Other Telegram Users**

Other users of our Services with whom you choose to communicate with and share certain information, who may be located outside the EEA. Note that by entering into the Terms of Service and choosing to communicate with such other users of Telegram, you are instructing us to transfer your personal data, on your behalf, to those users in accordance with this Privacy Policy. We employ all appropriate technical and organizational measures (including encryption of your personal data) to ensure a level of security for your personal data that is appropriate to the risk.

**8.2. Telegram’s Group Companies**

We may share your personal data with: *(1)* our parent company, Telegram Group Inc, located in the British Virgin Islands; and *(2)* Telegram FZ-LLC, a group member located in Dubai, to help provide, improve and support our Services. We will implement appropriate safeguards to protect the security and integrity of that personal data. This will take the form of standard contract clauses approved by the European Commission in an agreement between us and our relevant group companies. If you would like more information regarding these clauses, please contact us using the details in [section 12](https://telegram.org/privacy#12-questions-and-concerns) below.

**8.3. Law Enforcement Authorities**

If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened. When it does, we will include it in a semiannual transparency report published at: <https://t.me/transparency>.

**9. Your Rights Regarding the Personal Data You Provide to Us**

**9.1. Your Rights**

Under applicable data protection legislation, in certain circumstances, you have rights concerning your personal data. You have a right to: *(1)* request a copy of all your personal data that we store and to transmit that copy to another data controller; *(2)* delete (see [section 10](https://telegram.org/privacy#10-deleting-data) below) or amend your personal data; *(3)* restrict, or object to, the processing of your personal data; *(4)* correct any inaccurate or incomplete personal data we hold on you; and *(5)* lodge a complaint with national data protection authorities regarding our processing of your personal data.

**9.2. Exercising Your Rights**

If you wish to exercise any of these rights, kindly contact us using the details in [section 12](https://telegram.org/privacy#12-questions-and-concerns) below.

**9.3. Data Settings**

You can control how your data is used (e.g., delete synced contacts) in *Settings > Privacy & Security > Data Settings* (using one of our mobile apps).

Sadly, if you're generally not OK with Telegram's modest requirements, it won't be possible for us to provide you with our Services. You can delete your Telegram account by proceeding to the [deactivation page](https://telegram.org/deactivate).

**10. Deleting data**

**10.1. Accounts**

If you would like to delete your account, you can do this on the [deactivation page](https://telegram.org/deactivate). Deleting your account removes all messages, media, contacts and every other piece of data you store in the Telegram cloud. This action must be confirmed via your Telegram account and cannot be undone.

**10.2. Messages**

* In secret chats, deleting a message always instructs the app on the other end to delete it too.
* In cloud chats, you can choose to delete a message for all participants within at least 48 hours after sending. Otherwise, deleting a message will delete it from your message history. This means that a copy will stay on the server as part of your partner's message history. As soon as your partner deletes it too, it's gone forever.
* As of [version 5.5](https://telegram.org/blog/unsend-privacy-emoji), any party can choose to delete any messages in one-on-one chats, both sent and received, for both sides. There is no time limit. Any party can also opt to clear the entire chat history for both parties, in which case the apps will be instructed to remove all messages in that chat, however many of them are still retained by either of the participants.
* In [supergroups](https://telegram.org/blog/supergroups) and channels, deleting a message removes it for all participants. Note that deleted messages and original versions of edited messages from supergroups are stored for 48 hours after deletion in order to be shown in the [admins log](https://telegram.org/blog/admin-revolution#recent-admin-actions).

**10.3. Self-Destructing Messages**

Messages in Secret Chats can be ordered to [self-destruct](https://telegram.org/faq#q-how-do-self-destructing-messages-work). As soon as such a message is [read](https://telegram.org/faq#q-what-do-the-green-checks-mean) (2 checks appear), the countdown starts. When the timer expires, both devices participating in a secret chat are instructed to delete the message (photo, video, etc.). Media with short timers (less than a minute) are shown with blurred previews. The timer is triggered when they are viewed.

**10.4. Account Self-Destruction**

By default, if you stop using Telegram and do not come online for at least 6 months, your account will be deleted along with all messages, media, contacts and every other piece of data you store in the Telegram cloud. You can go to Settings to change the exact period after which your inactive account will self-destruct.

**11. Changes to this Privacy Policy**

We will review and may update this Privacy Policy from time to time. Any changes to this Privacy Policy will become effective when we post the revised Privacy Policy on this page [**www.telegram.org/privacy**](https://telegram.org/privacy). Please check our website frequently to see any updates or changes to our Privacy Policy, a summary of which we will set out below.

**March 25, 2019**

* Expanded [10.2. Deleting Messages] with data on the new features in [version 5.5](https://telegram.org/blog/unsend-privacy-emoji), which allow both participants to remove any messages from one-on-one chats for both sides without a time limit.

Important changes made to this Privacy Policy will be notified to you via Telegram.

**12. Questions and concerns**

If you have any questions about privacy and our data policies, please contact our [@GDPRbot](https://t.me/gdprbot). Use the */access* command to learn how to get a copy of your Telegram data and use the */contact* command to leave a request, which we will answer at the earliest opportunity.

Telegram is an open source project. You can examine more information on our:

* API at: <https://core.telegram.org/api>;
* Bot Platform at: <https://core.telegram.org/bots>;
* Protocol at: <https://core.telegram.org/mtproto>; and
* Source Code at: <https://telegram.org/apps#source-code>.

*This policy has been expanded on August 14, 2018 to add information required by the EU data protection law.*

King Games (Candy Crush Saga)

Privacy Policy

Use this option to keep a copy of this document

Formularbeginn

Print

Formularende

Intro

Hello! Welcome to the King Privacy Policy. This policy describes how King and, its other [group companies](https://king.com/groupCompanies) (collectively described as “King”, “we”, “us” or “our”) and its third party marketing and advertising partners collect, use, process and share information about you.

This Privacy Policy applies to all of our games, whether played on our website www.king.com, on mobile devices, PCs or on other platforms such as Facebook. It also applies to our Marketing and Advertising activities on all platforms and other services that we may provide to you from time to time. In this Privacy Policy we refer to our games, websites, marketing and advertising activities and other services collectively as our "Services".

By downloading, accessing and/or playing our games, or interacting with our websites or other Services, you agree to the collection and use of your information in accordance with this Privacy Policy, including consenting to King’s and our advertising partners’ use of your data for targeted advertising purposes as described in the Marketing and Advertising sections of this Privacy Policy. Those sections also explain how you can withhold or withdraw your consent to the use of your data for targeted advertising purposes. If you have any other concerns about providing information to us or it being used as described in this Privacy Policy you should not use our games or other Services.

Please note that this Privacy Policy does not apply when you use the Royal Games website (<http://www.royalgames.com/>).

This Privacy Policy was last updated on 7.9.2020.

Playing our games

By downloading, accessing and/or playing our games or using our other Services, you consent to the collection of information about you by us. Most of this data comes directly from you or your device, such as device information, country and region, and game play information. We use this data to provide our games and Services to you, including for the purposes of optimisation, preventing fraud, customising in-game offers and verifying purchases. We may also use it for the other purposes set out in this Privacy Policy, including for Marketing and Advertising purposes.

Find out more

Visiting our websites

When you visit our other websites, such as [https://community.king.com](https://community.king.com/), [https://candycrushsaga.com](https://candycrushsaga.com/), and other websites and forums operated by us (“Websites”), we collect information about you, such as details about how you use and interact with such Websites. We may use the information we collect about you for a number of purposes, including for operating and optimising the Websites, in connection with our advertising purposes, and for research or analysis.

Find out more

King Profile and Playing Socially

You can choose to add information to your King Profile or to connect our Services to your account with a third party network (such as Facebook). If you do this, then your personal information will be visible to other players and we’ll also use it for the other purposes set out in this Privacy Policy, including for Marketing and Advertising.

Find out more

Marketing

Unless you opt out as explained below, we and our third party partners use information collected about you to send you marketing communications about other King games and related Services based on your interests. For example, we may send emails, serve ads within our Services or place ads on third party websites, apps and Internet-connected devices.

Hide details

We may use the information that we hold about you to promote King’s or Activision Blizzard, Inc’s (“Activision Blizzard”) own Services in a number of ways. This might include:

* advertising within third party websites, apps and Internet-connect devices;
* showing you promotions for other King or Activision Blizzard games in the games you play; or
* sending you marketing materials by email.

What information do we use for marketing?

We use information about you to try to make sure you only see marketing from us that might be of interest to you. This includes using information that we may have about you, such as:

* ad identifiers and other non-personal information collected from your device. For more information, see Ad identifiers, cookies and similar technologies;
* the games you play and information about how you interact with our games and Services;
* your age, country or region, and gender; and
* other information that we might acquire from our third party marketing partners or other third parties who have obtained your consent or have another legal right to share that information with us.

Marketing partners

When we market our games in media published by other companies, we use various third party marketing partners to assist us on our behalf, and we may share information which we have collected about you with such third parties for these purposes.

Our marketing partners may help us to serve ads to you by combining this information with data which they have collected about you elsewhere. They collect this information when you use their services or the websites and services of third parties. Our partners use this information to make assumptions about the kinds of advertising you would prefer to see. If they determine that you would be interested to see an advert for King’s games or Services, they will serve you with a King ad while you are using other websites and services.

By accepting this Privacy Policy and downloading or continuing to play our games, and unless you opt out of interest-based advertising as explained in this section, you consent to our marketing partners collecting and using information about you to improve advertising, targeting and measurement systems as described in their privacy policies.

This Privacy Policy does not apply to the collection of your information by our marketing partners. We recommend that you review our partners’ privacy policies for more information. A list of our marketing partners and their privacy policies can be found [here](https://king.com/marketingPartners).

Opting-out of direct marketing from King

You can exercise choices over the direct marketing we send you in the following ways:

* you can withhold your consent for us to send you direct marketing emails by opting out when we collect your email address or by electing not to share your email address with us when you first create an account using your Facebook details;
* you can remove yourself from receiving email marketing from us at any time by simply clicking the unsubscribe link in any direct marketing email we send to you or sending an email to privacy@support.king.com; and
* to disable interest-based advertising, please see How to adjust your preferences for interest based advertising below.

You should note that if you opt out of receiving interest based or targeted advertising, you will still still see advertising and you may see advertising for King products, but that advertising will not be targeted using your personal information.

Advertising

Our games may include advertising for third party products and services.

King and our advertising partners collect and use information about you to improve advertising, targeting and measurement systems so that we can show you relevant third party ads in our games.

King participates in the IAB Europe Transparency & Consent Framework and complies with its Specifications and Policies. King uses the Consent Management Platform (CMP) with the identification number 28.

Where applicable, we use a CMP to gather consent and permissions for our advertising based activity. Where local laws allow, we may opt you into interest-based advertising by default. You can change your preferences at any time in the setting pages of our games.

Hide details

We use information that we hold about you to better target ads for third party goods and services to people that might be most interested in them. These ads may be shown to you within our games or Services.

What information is used for advertising?

We use ad identifiers and other information that we collect about you as described in this Privacy Policy to try to make sure you only see ads in our games that might be of interest to you. This includes information such as:

* ad identifiers and other information collected from your device. For more information, see Ad identifiers, cookies and similar technologies;
* the games you play and information about how you interact with our games and Services;
* your age, country and region, and gender; and
* other demographic and interests based information that we might acquire from our third party marketing partners or other third parties who have obtained your consent or have another legal right to share that information with us.

Advertising partners

When you play our games or use our Services, non-personal identifiers and other information from your device is collected and shared with advertising partners to enable the technical delivery of ads to your device.

Our advertising partners may combine this information with information which they have collected about you when you use their services (or the websites or services of third parties) in order to serve you more relevant ads in our games or to improve the accuracy of their targeting and measurement systems.

If you consent to, or are opted into, the collection and use of your data for targeted advertising purposes by our advertising partners your data will be used as set out in this section and as further described in our partners' privacy policies. We recommend that you review our advertising partners’ privacy policies for more information. A list of our advertising partners and their Privacy Policies can be found [here](https://king.com/advertisingPartners). You can refuse or withdraw your consent to such use at any time - for more information, see How to adjust your preferences for interest based advertising.

How to adjust your preferences for interest-based advertising

You can choose to prevent your device's ad identifier being used for interest-based advertising by updating the settings on your device.

If you opt out of interest-based advertising, you will still be able to play our games and you may still see advertising in our games, but those ads will not be targeted using information that we hold about you or which our advertising partners collect about you from our games (subject to the exclusion below for players not in California). However, you may still receive ads based on contextual criteria such as the game that the ad is displayed in, or the region in which your device is located.

For players in California: The California Consumer Privacy Act ("CCPA") gives residents of the US state of California the right to prevent businesses from selling their personal information to third parties. Please see the Advertising Partners section for more information on how we work with our advertising partners. Sharing information in this way may be considered “selling” for the purposes of the CCPA. We do not “sell” your personal information to third parties for any other purpose. If you would prefer that your personal information is not shared with third parties for this purpose, you can update your preferences in relevant games via the settings menu. If you wish to opt-out of this ‘selling’ of personal information in all our games, you can submit a “Do not sell my personal information” request here.

For players not in California: If you would prefer that your personal data is not processed to receive interest-based ads, you can update your preferences via the settings menu in relevant games. You can also submit an opt-out request for all of our games here. Please note that outside of California, even if you have opted-out of interest-based ads in our games, you may still receive interest-based ads from Facebook. If you would prefer that Facebook does not use your personal data for interest-based ads, you need to log into your account on Facebook and update your settings there.

Opting out of interest-based advertising at a device level: You can choose to prevent your device's ad identifier being used for interest-based advertising, or you can reset your device's ad identifier, by changing the settings of your device. Settings vary from device to device but you will usually find the ad identifier settings under "privacy" or "ads" in your device's settings. If you live in the USA, the EEA or Canada, you can also opt-out from the collection of your information by some or all of our advertising partners who participate in the Digital Advertising Alliance by visiting http://www.aboutads.info/choices/ (for US users), http://www.youronlinechoices.com/ (for EEA users) or http://youradchoices.ca/choices (for Canadian users). You can also click on the AdChoices logo within an advertisement (where available).

Ad identifiers, cookies and similar technologies

To provide our games, Websites and interest-based advertising, we use ad identifiers, cookies and similar technologies. This section describes our use of these technologies and how you can manage your preferences.

Hide details

Ad identifiers, cookies and similar technologies are used by us to provide our Services to you and in order to collect data from your device. These technologies allow us and our third party advertising partners to:

* recognise you and your device;
* provide interest-based advertising to you;
* allow our Services to interact with a third party social network or platform (where you have chosen to allow such interaction);
* allow us to understand how you interact with our websites (for example, where we use cookies such as the Google Analytics cookie on our Websites);
* allow our payment processors to process your payment instructions; and
* enable us and third parties to provide you with more customized services, for example to provide our Services in the correct language.

For more information on the cookies we use and why we use them, please see here.

How do ad identifiers, cookies and similar technologies work?

Ad identifiers are non-permanent, non-personal identifiers such as the Android advertising ID and/or Apple's ID for advertising (the ‘IDFA’), which are uniquely associated with your device. Similar technologies include tracking pixels within ads. These technologies allow companies (including marketers and advertisers) to recognise your device when you use websites and applications.

Cookies are small text files that are stored by your browser on your desktop computer or mobile device. You can withdraw your consent to cookies by updating the settings within your browser.

Your rights

You have certain rights in connection with your personal information and how we handle it. You can exercise these rights at any time by contacting us via any of the methods set out in the Contact Us section below.

Hide details

Those rights include:

* **Right of access.** You have a right to know what information we hold about you and in some cases to have the information communicated to you. If you wish to exercise this right please contact us letting us know that you wish to exercise your right of access and what information in particular you would like to receive. We reserve the right to ask for reasonable evidence to verify your identity before we provide you with any information. Please note that we may not be able to provide all the information you ask for, for instance if the information includes personal information about another person. Where we are not able to provide you with information that you have asked for, we will endeavour to tell you why.
* **Right to correct personal information.** We try to keep the information that we hold about you accurate and up to date. Should you realise that any of the information that we hold about you is incorrect, please let us know at privacy@support.king.com and we will correct it as soon as we can.
* **Data deletion.** In some circumstances you have a right to have some of the personal information that we hold about you deleted. Should you wish to have any information about you deleted, please Contact Us using the information below. Please note that in order to process your request you must delete our games from your mobile devices and clear our cookies from any device where you have played our games in a web browser. Where we delete personal information about you, we may still retain some or all of that information for other purposes such as maintaining financial records, protecting or enforcing legal rights, maintaining marketing suppression lists or for technical reasons such as maintaining technical security or our database integrity. We may also retain your information in an anonymised form. In some instances, personal information about you that is visible through gameplay such as username, avatar, your high scores and any chat messages may be cached on other players’ devices and we may not be able to remove or update that data from those devices, for example if that device is not connected to a wifi network.
* **Account deactivation.** If you have created an account with us, you can ask us to deactivate that account by contacting us using the information below. We may ask you for other information before we are able to deactivate your account. That information might include information about your mobile device. Other steps you should take should you wish to completely deactivate your account include disassociating your Facebook account from our mobile games and deleting our games from your mobile devices. Please note that if you completely deactivate your account all your progress in our games and any unspent virtual items, such as Gold Bars or Boosters will be lost and we may not be able to restore them in the future.
* **Data portability.** In some circumstances, you may have the right to request that data which you have provided to us is provided to you, so you can transfer this to another data controller.
* **Restriction of processing.** In some cases, you may have the right to request a restriction of the processing of your personal data, such as when you are disputing the accuracy of your data held by us.
* **Right to object.** You have the right to object to the processing of personal data about you which is processed on the grounds of legitimate interests (see Legal Bases below).
* **Direct marketing opt out.** If you have elected to receive direct marketing communications from us, you can change your mind at any time by following the opt out link in any marketing communication that is sent to you. If you have elected to receive more than one type of marketing communications from us, you may need to opt out of all of them individually. It may take a few days for us to update our records before any opt out is effective.
* **Right to opt-out (California, USA)**: California residents have the right to opt out of the sale of personal information, which is defined in a way that may include the transfer of data to third parties to personalize ads for you. If you opt out of the ‘sale’ of your information, we will not sell your information, including to our advertising partners, but you may still see ads in the game and some of our partners may deliver ads to you, based on information they hold on you. See How to adjust your preferences for interest-based advertising for more information.

There are other ways in which you can control the personal information that we collect about you. For instance, you could disconnect your Facebook or other social network account from our games, or delete our games from your mobile device. You could also reset your mobile advertising identifier or limit ad tracking altogether using the settings in your phone. Finally, you could limit or prevent the use of cookies in your web browsers. More information on all of these options is provided elsewhere in this Privacy Policy.

Children

You must be over a certain age to play our games and use our Services, depending on where you live. For the full list of age restrictions by country, please see below. We do not knowingly collect or solicit personal information from or direct or target interest based advertising to anyone under the ages set out below, or knowingly allow such persons to use our Services. If you believe that we might have any information from or about a child under the age set out below, please Contact Us.

Hide details

The table below sets out what age you must be to play our games and use our Services, depending on what country you are in while using our games and Services. Our games are intended to be played by adults and we do not knowingly collect, and do not wish to collect, information about children. Please do not play our games or use our Services if you are under the relevant age.

| Country | Age you must be to play our games and use our Services |
| --- | --- |
| Austria | 14 |
| Belgium | 13 |
| Bulgaria | 16 |
| Croatia | 16 |
| Republic of Cyprus | 14 |
| Czech Republic | 16 |
| Denmark | 13 |
| Estonia | 16 |
| Finland | 13 |
| France | 15 |
| Germany | 16 |
| Greece | 16 |
| Hungary | 16 |
| Ireland | 16 |
| Italy | 14 |
| Latvia | 13 |
| Lithuania | 14 |
| Luxembourg | 16 |
| Malta | 13 |
| Netherlands | 16 |
| Norway | 13 |
| Poland | 16 |
| Portugal | 16 |
| Romania | 16 |
| Slovakia | 16 |
| Slovenia | 16 |
| Spain | 14 |
| Sweden | 13 |
| Switzerland | 16 |
| United Kingdom | 13 |
| Rest of the world (excluding South Korea) | 13 |

If you believe that we might have any information from or about a child under the relevant age set out above, please Contact Us. In the event that we learn that we have collected personal information from a child under the relevant age set out above, we will delete that information as quickly as possible.

General

Our Privacy Policy contains further details about:

* who we share your information with and the reasons for sharing it;
* measures we take to keep your information secure;
* the legal bases under which we process your data;
* how long we retain your information and where we store it;
* when and why we share your information with third parties, including transfers outside of the European Economic Area (the “EEA”); and
* changes or updates to our Privacy Policy.

Hide details

Sharing

In addition to the other disclosures described in this Privacy Policy, we will also share your information:

* where we have your consent to do so (including as set out in this Privacy Policy);
* as reasonably necessary in order to provide the Services to you (for example, by providing your personal information to suppliers we may use to fulfil the Services or to communicate with you);
* where it is necessary to carry out your instructions (for example, to process a payment instruction we must provide your personal information to our payment processors);
* where your data is in an anonymous and aggregated format, meaning you could not be personally identified from it;
* as we reasonably believe is permitted by law or regulation or as is necessary to comply with any legal obligation, or in order to enforce or apply our terms and conditions and/or any other agreement with you; or to protect the rights, property, or safety of King, our users, or others; and
* if there is a sale of the assets of King or corporate restructuring, or as a result of a change of control of King or one of its group companies, or in preparation of any of these events. Any third party to which King transfers of sells King's assets will have the right to continue to use the personal and other information that you provide to us in the manner set out in this Privacy Policy.

We may also share your information with our service providers if necessary to enable them to provide services to us.

Security

King takes appropriate security and technical measures to protect your information from unauthorised access, loss and misuse. In addition, we request that our suppliers who process personal information on our behalf take a range of security measures designed to help protect your personal information and maintain an appropriate level of security. However, we cannot guarantee the absolute security of your information online and offline, as the Internet by its nature is not a secure environment and the nature of security risks is constantly evolving. As such you should always take care when sharing your information online.

Legal Bases

In each case where we process your information, we do so lawfully in accordance with one of the legal basis set out under European data protection law. The legal bases which we rely upon are the following:

* **Contractual Necessity.** This covers data used by us in order to provide you with Services that you have requested - and that we have agreed - to provide to you, such as our games, customer services, chat functionality and third party social network connectivity;
* **Legal Obligation.** This covers data used by us to comply with a legal obligation, such as to maintain records relating to tax or to respond to a valid legal request for certain data;
* **Legitimate Interests.** This covers data used by us for purposes that are not harmful to your privacy and can be reasonably expected within the context of your use of our Services, such as Marketing, Advertising, analytics, research and optimisation of our games and other Services; and
* **Consent.** This is used as a legal basis in the following contexts: (i) the collection of data stored on your device by us and our advertising partners, including device information, ad identifiers, IP address, country and region. You consent to this collection when you agree to install our game and you can withdraw your consent to this by uninstalling our games; (ii) the storage of data on your device by us and our advertising partners, including through the use of cookies. By accessing and using our Services, you consent to this storage and you can withdraw your consent by updating your cookie settings; and (iii) the use of your data by us and our partners for targeted advertising purposes (for more information, see Marketing and Advertising above). You consent to this collection when you accept this Privacy Policy and you can withdraw your consent to this processing by following the steps at How to adjust your preferences for interest based advertising. Where we ask for your consent to use your data for any other purpose, we will make this clear at the point of collection and we will also make clear how you can withdraw your consent.

In this Privacy Policy we have explained how you can opt out of certain types of processing that we undertake and where any processing is based on your consent, you can withdraw that consent at any time in the ways described in this Privacy Policy. Nonetheless, if you play our games we will still collect some personal data about you and process it as otherwise described in this Privacy Policy. If you do not wish us to collect any personal data about you at all, you should cease playing our games and stop using our Services.

Retention

We will keep your information for as long as your account is active or we consider necessary for the purposes described in our Privacy Policy. We will also retain and use your information for as long as is required in order to comply with our legal obligations.

Location of storage

We store your information on servers that we control which are primarily based in the EEA. We may also use servers and engage providers that are located outside the EEA in order to process and store your information and to provide services to us.

International Transfer

We may transfer your information to affiliated entities or third parties to jurisdictions outside the EEA. Please note that these countries outside of the EEA may not have the same data protection laws as your own jurisdiction. We take steps to ensure that there are adequate safeguards and mechanisms in place (including the use of EU model clauses) to allow the transfer of your information across borders outside of the EEA.

South Korea

Please note that a different version of this Privacy Policy applies if you live in South Korea (please see [https://king.com/ko/privacyPolicy](https://www.king.com/ko/privacyPolicy)).

Changes to this Privacy Policy

We may update this Privacy Policy from time to time and we will post the updated Privacy Policy on this page. Please come back to this page every now and then to make sure you are familiar with the latest version. Any new policy will be effective from the date it is published by us.

Contact us

If you have any questions or concerns about any of the matters in relation to this Privacy Policy, including to exercise any of your rights, then there are several way of contacting us:

1. via our customer services page at <https://soporto.king.com/contact>;
2. via email to [privacy@support.king.com](mailto:privacy@support.king.com); or
3. in writing to King.com Ltd of Aragon House Business Centre, Level 4, Dragonara Road, St Julians STJ3140, Malta.

For information collected under this Privacy Policy, the data controller is King.com Limited. Our Data Protection Officer can be contacted here: dataprotectionofficer@king.com.

Snapchat US

Privacy Policy

Effective: September 14, 2020

Snap Inc. is a camera company. Our products and services—including Snapchat, Bitmoji, Spectacles, advertising, and others that link to this Privacy Policy—provide fast and fun ways to express yourself, live in the moment, learn about the world, and have fun together!

When you use these services, you’ll share some information with us. So we want to be upfront about the information we collect, how we use it, whom we share it with, and the controls we give you to access, update, and delete your information.

That’s why we’ve written this Privacy Policy. And it’s why we’ve tried to write it in a way that’s blissfully free of the legalese that often clouds these documents. Of course, if you still have questions about anything in our Privacy Policy, just [contact us](https://support.snapchat.com/).

You should read our entire Privacy Policy, but when you only have a few minutes or want to remember something later on, you can always take a look at [this summary](https://www.snap.com/privacy/your-privacy/)—so you can review some of the basics in just a few minutes.

**Information We Collect**

There are three basic categories of information we collect:

* **Information you provide.**
* **Information we get when you use our services.**
* **Information we get from third parties.**

Here’s a little more detail on each of these categories.

**Information You Provide**

When you interact with our services, we collect information that you provide to us. For example, most of our services require you to set up a Snapchat account, so we need to collect a few important details about you, such as your name, username, password, email address, phone number, and date of birth. We may also ask you to provide us with some additional information that will be publicly visible on our services, such as a profile picture or Bitmoji avatar. Other services, such as commerce products, may require you to provide us with a debit or credit card number and its associated account information.

Of course, you’ll also provide us whatever information you send through our services, such as Snaps and Chats. Keep in mind that the users who view your Snaps, Chats, and any other content can always save that content or copy it outside the app. So, the same common sense that applies to the internet at large applies to Snapchat as well: Don’t send messages or share content that you wouldn’t want someone to save or share.

When you contact customer support or communicate with us in any other way, we’ll collect whatever information you volunteer or that we need to resolve your question.

**Information We Get When You Use Our Services**

When you use our services, we collect information about which of those services you’ve used and how you’ve used them. We might know, for instance, that you watched a particular Story, saw a specific ad for a certain period of time, and sent a few Snaps. Here’s a fuller explanation of the types of information we collect when you use our services:

* **Usage Information.** We collect information about your activity through our services. For example, we may collect information about:
  + how you interact with our services, such as which filters you view or apply to Snaps, which Stories you watch on Discover, whether you’re using Spectacles, or which search queries you submit.
  + how you communicate with other Snapchatters, such as their names, the time and date of your communications, the number of messages you exchange with your friends, which friends you exchange messages with the most, and your interactions with messages (such as when you open a message or capture a screenshot).
* **Content Information.** We collect content you create on our services, such as custom stickers, and information about the content you create or provide, such as if the recipient has viewed the content and the metadata that is provided with the content.
* **Device Information.** We collect information from and about the devices you use. For example, we collect:
  + information about your hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone;
  + information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether you have headphones connected; and
  + information about your wireless and mobile network connections, such as mobile phone number, service provider, IP address, and signal strength.
* **Device Phonebook.** Because Snapchat is all about communicating with friends, we may—with your permission—collect information from your device’s phonebook.
* **Camera and Photos.** Many of our services require us to collect images and other information from your device’s camera and photos. For example, you won’t be able to send Snaps or upload photos from your camera roll unless we can access your camera or photos.
* **Location Information.** When you use our services we may collect information about your location. With your permission, we may also collect information about your precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses.
* **Information Collected by Cookies and Other Technologies.** Like most online services and mobile applications, we may use cookies and other technologies, such as web beacons, web storage, and unique advertising identifiers, to collect information about your activity, browser, and device. We may also use these technologies to collect information when you interact with services we offer through one of our partners, such as advertising and commerce features. For example, we may use information collected on other websites to show you more relevant ads. Most web browsers are set to accept cookies by default. If you prefer, you can usually remove or reject browser cookies through the settings on your browser or device. Keep in mind, though, that removing or rejecting cookies could affect the availability and functionality of our services. To learn more about how we and our partners use cookies on our services and your choices, please check out our [Cookie Policy](https://www.snap.com/en-US/cookie-policy/).
* **Log Information.** We also collect log information when you use our website, such as:
  + details about how you’ve used our services;
  + device information, such as your web browser type and language;
  + access times;
  + pages viewed;
  + IP address;
  + identifiers associated with cookies or other technologies that may uniquely identify your device or browser; and
  + pages you visited before or after navigating to our website.

**Information We Collect from Third Parties**

We may collect information about you from other users, our [affiliates](https://support.snapchat.com/a/snap-affiliates), and third parties. Here are a few examples:

* If you link your Snapchat account to another service (like Bitmoji or a third-party app), we may receive information from the other service, like how you use that service.
* Advertisers, app developers, publishers, and other third parties may share information with us as well. We may use this information, among other ways, to help target or measure the performance of ads. You can learn more about our use of this kind of third-party data in our [Support Center](https://support.snapchat.com/a/advertising-preferences).
* If another user uploads their contact list, we may combine information from that user’s contact list with other information we have collected about you.

**How We Use Information**

What do we do with the information we collect? For the detailed answer, go [here](https://www.snap.com/privacy/your-information). The short answer is: Provide you with an amazing set of products and services that we relentlessly improve. Here are the ways we do that:

* develop, operate, improve, deliver, maintain, and protect our products and services.
* send you communications, including by email. For example, we may use email to respond to support inquiries or to share information about our products, services, and promotional offers that we think may interest you.
* monitor and analyze trends and usage.
* [personalize our services](https://www.snap.com/privacy/privacy-by-product#personalization) by, among other things, suggesting friends, profile information, or Bitmoji stickers, or customizing the content we show you, including ads.
* contextualize your experience by, among other things, tagging your Memories content using your precise location information (if, of course, you’ve given us permission to collect that information) and applying other labels based on the content.
* provide and improve our advertising services, ad targeting, and ad measurement, including through the use of your precise location information (again, if you’ve given us permission to collect that information), both on and off our services. See the [Control Over Your Information](https://www.snap.com/en-US/privacy/privacy-policy#control-over-your-information) section below for more information about Snap Inc.’s advertising practices and your choices.
* enhance the safety and security of our products and services.
* verify your identity and prevent fraud or other unauthorized or illegal activity.
* use information we’ve collected from cookies and other technology to enhance our services and your experience with them.
* enforce our Terms of Service and other usage policies and comply with legal requirements.

We may also use information from Apple’s TrueDepth camera to improve the quality of Lenses. Information from the TrueDepth camera is used in real time—we don’t store this information on our servers or share it with third parties.

**How We Share Information**

We may share information about you in the following ways:

* **With other Snapchatters.** We may share the following information with other Snapchatters:
  + information about you, such as your username, name, and Bitmoji.
  + information about how you have interacted with our services, such as your Snapchat “score,” the names of Snapchatters you are friends with, and other information that will help Snapchatters understand your connections with others using our services. For example, because it may not be clear whether a new friend request comes from someone you actually know, we may share whether you and the requestor have Snapchat friends in common.
  + any additional information you have directed us to share. For example, Snap will share your information when you connect your Snapchat account to a third-party app, and if you share information or content from Snapchat to the third-party app.
  + content you post or send. How widely your content is shared depends on your personal settings and the type of service you are using. For example, a Snap may be sent to just a single friend you select, but your My Story content may be seen by any Snapchatter whom you allow to see your My Story.
* **With all Snapchatters, our business partners, and the general public.** We may share the following information with all Snapchatters as well as with our business partners and the general public:
  + public information like your name, username, Snapcode and profile pictures.
  + Story submissions that are set to be viewable by Everyone and any content that you submit to an inherently public service, like Our Story and other crowd-sourced services. This content may be viewed and shared by the public at large both on and off our services, including through search results, on websites, in apps, and in online and offline broadcasts.
* **With our affiliates.** We may share information with entities within the [Snap Inc. family of companies](https://support.snapchat.com/a/snap-affiliates).
* **With third parties.** We may share information about you with service providers who perform services on our behalf, including to measure and optimize the performance of ads and deliver more relevant ads, including on third-party websites and apps. Learn more [here](https://support.snapchat.com/a/snapchat-service-providers).
  + We may share information about you with business partners that provide services and functionality on our services. For more information about information collected by third parties on our services, visit our [Support Site](https://support.snapchat.com/article/integrated-features).
  + We may share information about you, such as device and usage information, to help us and others prevent fraud.
  + We may share information about you for legal, safety, and security reasons. We may share information about you if we reasonably believe that disclosing the information is needed to:
    - comply with any valid legal process, governmental request, or applicable law, rule, or regulation.
    - investigate, remedy, or enforce potential Terms of Service violations.
    - protect the rights, property, or safety of us, our users, or others.
    - detect and resolve any fraud or security concerns.
  + We may share information about you as part of a merger or acquisition. If Snap Inc. gets involved in a merger, asset sale, financing, liquidation or bankruptcy, or acquisition of all or some portion of our business to another company, we may share your information with that company before and after the transaction closes.

We may also share with third parties that provide services to us or perform business purposes for us aggregated, non-personally identifiable, or de-identified information.

**Third-Party Content and Integrations**

Our services may contain third-party content and integrations. Examples include third-party integrations in camera search, third-party games in Chat, and third-party Snap Kit integrations. Through these integrations, you may be providing information to the third party as well as to Snap. We are not responsible for how those third parties collect or use your information. As always, we encourage you to review the privacy policies of every third-party service that you visit or use, including those third parties you interact with through our services. You can learn more about third-party services in Snapchat [here](https://support.snapchat.com/article/integrated-features).

**How Long We Keep Your Information**

Snapchat lets you capture what it’s like to live in the moment. On our end, that means most messages—like Snaps and Chats—sent in Snapchat will be automatically deleted by default from our servers after we detect they’ve been opened by all recipients or have expired. Other content, like Story posts, are stored for longer. For detailed information about how long we store different types of content, check out our [Support Site](https://support.snapchat.com/article/when-are-snaps-chats-deleted).

We store other information for longer periods of time. For example:

* We store your basic account information—like your name, phone number, and email address—and list of friends until you ask us to delete them.
* We store location information for different lengths of time based on how precise it is and which services you use. For example, if you use the Map, we store information about your favorite places for up to 40 days so we can personalize and improve your experience. If location information is associated with a Snap—like those saved to Memories or posted to Our Story—we’ll retain that location as long as we store the Snap.
* We’re constantly collecting and updating information about the things you might like and dislike, so we can provide you with more relevant content and advertisements. Go [here](https://support.snapchat.com/a/advertising-preferences) to learn more.

If you ever decide to stop using Snapchat, you can just [ask us to delete your account](https://support.snapchat.com/a/delete-my-account1). We’ll also delete most of the information we’ve collected about you after you’ve been inactive for a while—but don’t worry, we’ll try to contact you first!

Keep in mind that, while our systems are designed to carry out our deletion practices automatically, we cannot promise that deletion will occur within a specific timeframe. There may be legal requirements to store your data and we may need to suspend those deletion practices if we receive valid legal process asking us to preserve content, if we receive reports of abuse or other Terms of Service violations, or if your account or content created by you is flagged by our automated systems for abuse or other Terms of Service violations. Finally, we may also retain certain information in backup for a limited period of time or as required by law.

**Control Over Your Information**

We want you to be in control of your information, so we provide you with the following tools.

* **Access, Correction, and Portability.** You can access and edit most of your basic account information right in our apps. You can also use [Download My Data](https://accounts.snapchat.com/accounts/downloadmydata) to obtain a copy of information that isn’t available in our apps in a portable format, so you can move it or store it wherever you want. Because your privacy is important to us, we will ask you to verify your identity or provide additional information before we let you access or update your personal information. We may also reject your request to access or update your personal information for a number of reasons, including, for example, if the request risks the privacy of other users or is unlawful.
* **Revoking permissions.** In most cases, if you let us use your information, you can simply revoke your permission by changing the settings in the app or on your device if your device offers those options. Of course, if you do that, certain services may lose full functionality.
* **Deletion.** While we hope you’ll remain a lifelong Snapchatter, if for some reason you ever want to delete your account, just go [here](https://support.snapchat.com/a/delete-my-account1) to learn how. You can also delete some information in the app, like photos you’ve saved to Memories, Our Story submissions, and search history.
* **Advertising Preferences.** We try to show you ads that we think will be relevant to your interests. If you would like to modify the information we and our advertising partners use to select these ads, you can do so in the app and through your device preferences. Go [here](https://support.snapchat.com/a/advertising-preferences) to learn more.
* **Communicating with other Snapchatters.** It’s important to us that you stay in control over whom you communicate with. That’s why we’ve built a number of tools in Settings that let you indicate, among other things, who you want to see your Stories, whether you’d like to receive Snaps from just your friends or all Snapchatters, and whether you’d like to block another Snapchatter from contacting you again. Go [here](https://support.snapchat.com/article/privacy-settings2) to learn more.

**Users in the European Union**

If you’re a user in the European Union, you should know that Snap Inc. is the controller of your personal information. Here is some additional information we would like to bring to your attention:

**Rights of Access, Deletion, Correction, and Portability**

You can exercise your rights of access, deletion, correction, and portability as described in the [Control Over Your Information](https://www.snap.com/en-US/privacy/privacy-policy#control-over-your-information) section above.

**Bases for Using Your Information**

Your country only allows us to use your personal information when certain conditions apply. These conditions are called “legal bases” and, at Snap, we typically rely on one of four:

* **Contract.** One reason we might use your information is because you’ve entered into an agreement with us. For example, when you buy an On-Demand Geofilter and accepted our Custom Creative Tools Terms, we need to use some of your information to collect payment and make sure we show your Geofilter to the right people at the right place and time.
* **Legitimate interest.** Another reason we might use your information is because we have—or a third party has—a legitimate interest in doing so. For example, we need to use your information to provide and improve our services, including protecting your account, delivering your Snaps, providing customer support, and helping you find friends and content we think you’ll like. Because most of our services are free, we also use some information about you to try and show you ads you’ll find interesting. An important point to understand about legitimate interest is that our interests don’t outweigh your right to privacy, so we only rely on legitimate interest when we think the way we are using your data doesn’t significantly impact your privacy or would be expected by you, or there is a compelling reason to do so. We explain our legitimate business reasons for using your information in more detail [here](https://www.snap.com/privacy/your-information).
* **Consent.** In some cases we’ll ask for consent to use your information for specific purposes. If we do, we’ll make sure you can revoke your consent in our services or through your device permissions. Even if we’re not relying on consent to use your information, we may ask you for permission to access data like contacts and location.
* **Legal obligation.** We may be required to use your personal information to comply with the law, like when we respond to valid legal process or need to take action to protect our users. Our policy is to notify Snapchatters when we receive legal process seeking their account information, with some exceptions. Learn more [here](https://www.snap.com/privacy/transparency/).

**Your Right to Object**

You have the right to object to our use of your information. With many types of data, we’ve provided you with the ability to simply delete it if you don’t want us processing it anymore. For other types of data, we’ve given you the ability to stop the use of your data by disabling the feature altogether. You can do these things in the app. If there are other types of information you don’t agree with us processing, you can [contact us](https://support.snapchat.com/).

**International Transfers**

We may collect your personal information from, transfer it to, and store and process it in the United States and other countries outside of where you live. Whenever we share information of EU users outside the EU we make sure an adequate transfer mechanism is in place. You can find more information on the categories of third parties we share information with [here](https://support.snapchat.com/a/snapchat-service-providers).

**Complaints?** If you’re based in the EU, you can always file a complaint with the [supervisory authority](https://edpb.europa.eu/about-edpb/board/members_en) in your Member State.

**Users in Brazil**

If you’re a user in Brazil you should know that Snap Inc. is the controller of your personal information. Here is some additional information we would like to bring to your attention:

**Rights of Access, Deletion, Correction, and Portability**

You can exercise your rights of access, deletion, correction, and portability as described in the Control Over Your Information section above.

**Bases for Using Your Information**

Your country only allows us to use your personal information when certain conditions apply. These conditions are called “legal bases” and, at Snap, we typically rely on one of four:

* Contract. One reason we might use your information is because you’ve entered into an agreement with us. For example, when you buy an On-Demand Geofilter and accepted our Custom Creative Tools Terms, we need to use some of your information to collect payment and make sure we show your Geofilter to the right people at the right place and time.
* Legitimate interest. Another reason we might use your information is because we have—or a third party has—a legitimate interest in doing so. For example, we need to use your information to provide and improve our services, including protecting your account, delivering your Snaps, providing customer support, and helping you find friends and content we think you’ll like. Because most of our services are free, we also use some information about you to try and show you ads you’ll find interesting. An important point to understand about legitimate interest is that our interests don’t outweigh your right to privacy, so we only rely on legitimate interest when we think the way we are using your data doesn’t significantly impact your privacy or would be expected by you, or there is a compelling reason to do so. We explain our legitimate business reasons for using your information in more detail here.
* Consent. In some cases we’ll ask for consent to use your information for specific purposes. If we do, we’ll make sure you can revoke your consent in our services or through your device permissions. Even if we’re not relying on consent to use your information, we may ask you for permission to access data like contacts and location.
* Legal obligation. We may be required to use your personal information to comply with the law, like when we respond to valid legal process or need to take action to protect our users.

**Your Right to Object**

You have the right to object to our use of your information. With many types of data, we’ve provided you with the ability to simply delete it if you don’t want us processing it anymore. For other types of data, we’ve given you the ability to stop the use of your data by disabling the feature altogether. You can do these things in the app. If there are other types of information you don’t agree with us processing, you can contact us.

**Complaints?** You can always file a complaint with the national authority in your country. Additionally, we have appointed a Data Protection Officer (“DPO”). To contact our DPO, please email dpo @ snap.com.

**Users in Mexico**

If you’re a user in Mexico, you should know that Snap Inc., located at 2772 Donald Douglas Loop North, Santa Monica, California 90405, is the controller of your personal information. Here is some additional information we would like to bring to your attention:

**Rights of Access, Rectification, and Cancellation**

You can exercise your rights of access, rectification, and cancellation as described in the Control Over Your Information section above.

**Your Right to Object or Challenge**

You have the right to object to or challenge our use of your information. With many types of data, we’ve provided you with the ability to simply delete it if you don’t want us processing it anymore. For other types of data, we’ve given you the ability to stop the use of your data by disabling the feature altogether. You can do these things in the app. If there are other types of information you don’t agree with us processing, you can [contact us](https://support.snapchat.com/en-US).

**California Residents**

If you’re a California resident, you have certain privacy rights under California law, including the California Consumer Privacy Act of 2018 (“CCPA”). Our California Privacy Notice specifies these rights, [check it out](https://www.snap.com/privacy/california-privacy-notice).

**Children**

Our services are not intended for—and we don’t direct them to—anyone under 13. And that’s why we do not knowingly collect personal information from anyone under 13. In addition, we may limit how we collect, use, and store some of the information of EU users between 13 and 16. In some cases, this means we will be unable to provide certain functionality to these users. If we need to rely on consent as a legal basis for processing your information and your country requires consent from a parent, we may require your parent’s consent before we collect and use that information.

**Revisions to the Privacy Policy**

We may change this Privacy Policy from time to time. But when we do, we’ll let you know one way or another. Sometimes, we’ll let you know by revising the date at the top of the Privacy Policy that’s available on our website and mobile application. Other times, we may provide you with additional notice (such as adding a statement to our websites’ homepages or providing you with an in-app notification).

ScoopWhoop

**Privacy policy**

1. **INTRODUCTION**
   1. Your privacy and trust are important to us. ‘ScoopWhoop Media Private Limited’, a company incorporated under the laws of India, having its registered office at ‘C-5, Green Avenue Street, Church Road, Vasant Kunj, New Delhi - 110 070’, - the term includes ‘ScoopWhoop Media Private Limited’s subsidiary/ies, affiliate/s, channel/s, joint venture/s, sister concern/s, franchise/s et cetera. (hereinafter collectively referred to as “ScoopWhoop”, “we”, “us” or “our”), which operates various websites, applications, softwares, products and other services including but not limited to delivery of information and content via any internet connected device – computer, laptop, tablet, mobile or otherwise (hereinafter collectively referred to as “Services”).
   2. This Policy explains how ScoopWhoop collects, handles, stores and protects personal information about you in the context of our services. It also provides information about your rights and about how you can contact us if you have questions about how we handle your information. This Policy applies to individuals who use our services through any medium, inter alia, website, application, our or third party social media pages, any other electronic communication et cetera. This policy DOES NOT apply to information that you provide to, or that is collected by, any third-party, for the purposes of tracking ‘user behavior’. ScoopWhoop encourages you to consult directly with such third-parties about their privacy practices.
   3. We care about the privacy of our users, such as yourself. We respect the information that you provide to us, and want to be sure you fully understand exactly how we use that information. By accepting to access our website at [insert all links here], you are also agreeing to this privacy policy (hereinafter referred to as “Privacy Policy”).
   4. Please read this policy carefully to understand ScoopWhoop's policies and practices regarding your information and how ScoopWhoop will treat it. By accessing or using our Services, you agree to this Privacy Policy and you are consenting to ScoopWhoop's collection, use, disclosure, retention, and protection of your Information (Personal Information and/or Sensitive Personal Data or Information), as described here. If you do not wish to agree with terms of our Privacy Policy, we kindly request you not to, in any manner, use our services through any medium, inter alia, website, application, our or third party social media pages, any other electronic communication et cetera.
2. **THE INFORMATION WE COLLECT AND HOW WE USE IT**
   1. ScoopWhoop collects several types of information from and about users of our Services, including:
      1. Your Personal Information - the information that can be associated with a specific person and could be used to identify that specific person whether from that data, or from the data and other information that we have, or is likely to have access to. We do not consider personal information to include information that has been made anonymous or aggregated so that it can no longer be used to identify a specific person, whether in combination with other information or otherwise.
      2. Information about your internet connection, the equipment you use to access our Services and your usage details.
   2. We collect this information:
      1. directly from you when you provide it to us, especially when you login through other social media website login interface, for the purposes of accessing NSFW (Not safe for work) articles which require adult age consent; and/or
      2. automatically as you navigate through our Services (information collected automatically may include usage details, IP addresses and information collected through cookies, web beacons and other tracking technologies).
3. **INFORMATION YOU PROVIDE TO US**

The information we collect on or through our Services may include:

* 1. **Your account information:** Your full name, email address, postal code, user id, password and other information that you may provide or have provided with your account on third party platforms and collated by us through third-party sign-in services such as Facebook and Google Plus, such as your gender, mobile phone number and website.
  2. **Your preferences:** Your preferences and settings saved on third-party sign-in services websites such as time zone and language.
  3. **Your content:** Information you provide through our Services, including your likes, shares, comments, other details and history, favorites; specific contact information of people you add to, or notify of, our Services, names, and other information you provide on our Services, and other information in your account profile.
  4. **Your searches and other activities:** The search terms you have looked up and results you selected.
  5. **Your browsing information:** How long you used our Services and which features you used; the advertisements you clicked on.
  6. **Your communications:** Communications between you and other users or third party links or advertisements through our Services; your participation in a survey, poll, contest or promotion scheme; your request for certain features (e.g., newsletters, updates or other services); your communication with us about employment opportunities posted to the services.
  7. **Your Public Posts:** You also may provide information (such as comments, likes, bookmarks, friends, lists, etc.) to be published or displayed or posted (hereinafter, "posted") on publicly accessible areas of our Services, or transmitted to other users of our Services or third-parties (collectively, "User Contributions"). Your User Contributions are posted on and transmitted to others at your own risk. Please be aware that we cannot control the actions of other users of our Services with whom you may choose to share your User Contributions. Therefore, we cannot and do not guarantee that your User Contributions will not be viewed by unauthorized persons.

1. **INFORMATION WE COLLECT THROUGH AUTOMATIC DATA COLLECTION TECHNOLOGIES**

We may automatically collect certain information about the computer or devices (including mobile devices) you use to access the Services, and about your use of the Services, even if you use the Services without registering or logging in.

* 1. **Usage information:** Details of your use of our Services, including traffic data, location data, time zone, language preference, logs and other communication data and the resources that you access and use on or through our Services.
  2. **Computer and device information:** Information about your computer, Internet connection and mobile device, including your IP address, operating systems, platforms, browser type, other browsing information (connection, speed, connection type etc.), device type, device's unique device identifier, mobile network information and the device's telephone number.
  3. **Stored information and files:** We may also access metadata and other information associated with other files stored on your device. This may include, for example, photographs, audio and video clips, personal contacts and address book information.
  4. **Last URL visited:** The URL of the last web page you visited before visiting our websites.
  5. **Mobile device IDs:** Unique mobile device identifier (e.g. IDFA or other device IDs on Apple devices like the iPhone and iPad), if you're using our Services on a mobile device, we may use mobile device IDs (the unique identifier assigned to a device by the manufacturer), instead of cookies, to recognize you. We may do this to store your preferences and track your use of our website. Unlike cookies, mobile device IDs cannot be deleted. Advertising companies may use device IDs to track your use of our website, track the number of advertisements displayed, measure advertising performance and display advertisements that are more relevant to you. Analytics companies may use mobile device IDs to track your usage of our services .
  6. **Your activity on the Services:** Information about your activity on the Services, such as your search queries, comments, domain names, search results selected, number of clicks, pages viewed and the order of those pages, how long you visited our Services, the date and time you used the Services, error logs, and other similar information.

1. **COOKIES AND OTHER ELECTRONIC TOOLS**
   1. We, and third parties with whom we partner, may use cookies, pixel tags, web beacons, mobile device IDs, "flash cookies" and similar files or technologies to collect and store information in respect to your use of the Services and third party websites. A cookie is a small text file that is stored on your computer that enables us to recognize you when you visit our website, store your preferences and settings, enhance your experience by delivering content and advertising specific to your interests (tailored advertising), perform research and analytics (internal and/or through third party), track your use of our Services, and assist with security and administrative functions.
   2. Most browsers are set to automatically allow cookies. Please note it may be possible to disable some (but not all) cookies through your device or browser settings, but doing so may interfere with certain functionality on the Services. You may also alter your settings to receive alert notifications when cookies are being sent. To modify your cookie settings, please visit your browser's help settings. You will need to opt out on each browser and each device you use to access the Services. By using our Services with your browser set to accept cookies you are consenting to our use of cookies.
   3. Third parties whose products or services are accessible or advertised through the Services, including social media services, may also use cookies or similar tools, and we advise you to check their privacy policies for information about their cookies and other practices. We do not control the practices of such partners and their privacy policies govern their interactions with you.
2. **USE OF THE INFORMATION COLLECTED**

We use the information we collect from and about you for legitimate purposes, inter alia, to:

* 1. Understand our users (what they do on our Services, what features they like, how they use them, etc.), improve the content and features of our Services (such as by personalizing content to your interests); process and respond to your queries; send you communications that you have requested and/or notifications/updates/pop-ups; provide you with support service; et cetera.
  2. Administer our Services and diagnose technical problems.
  3. Enable us to show you ads that are relevant to you.
  4. Generate and review reports and data about, and to conduct research on, our user base and Service usage patterns.
  5. Carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for remuneration.
  6. Enable us to display advertisements to our advertisers'/service providers' target audiences. Even though we do not disclose your personal information for these purposes without your consent, if you click on or otherwise interact with an advertisement, the advertiser may assume that you meet its target criteria.

1. **SHARING OF THE INFORMATION COLLECTED**

We may disclose personal information that we collect or you provide, as described in this privacy policy, in the following ways:

* 1. Internally, to our subsidiaries and affiliates and sister concerns;
  2. To contractors, advertisers/service providers and other third-parties;
  3. To third-parties to market their products or services to you if you have consented to receive the promotional updates. We contractually require these third-parties to keep personal information confidential and use it only for the purposes for which we disclose it to them.
  4. We may share your information with outside vendors that we use for a variety of purposes, such as to send you communications via emails to inform you about our services that may be of interest to you, push notifications/pop-ups to your devices on our behalf et cetera.
  5. **Legal Purposes.** We may share your information when we believe in good faith that such sharing is reasonably necessary in order to investigate, prevent, or take action regarding possible illegal activities or to comply with legal process. We may also share your information to investigate and address threats or potential threats to the physical safety of any person, to investigate and address violations of this Privacy Policy or to investigate and address violations of the rights of third parties and/or to protect the rights, property and safety of ScoopWhoop, our employees, users, or the public. This may involve the sharing of your information with law enforcement, government agencies, courts, and/or other organizations on account of legal request such as subpoena, court order or government demand to comply with the law.
  6. **Social Networks.** If you interact with social media features on our Services, such as the Facebook Like button, or use your social media credentials to log-in or post content, these features may collect information about your use of the Services, as well as post information about your activities on the social media service. Your interactions with social media companies are governed by their privacy policies.
  7. **Consent.** We may share your information in any other circumstances where we have your consent.

1. **CHANGES THROUGH YOU**
   1. When you sign up or make request for certain features (e.g., newsletters, updates or any other services), you are opting in to receive emails/notifications/pop-ups from ScoopWhoop including its allied concerns. You can log in to manage your email preferences and follow the "unsubscribe" instructions in commercial email messages, but note that you cannot opt out of receiving certain administrative policy, service policy, or legal policy email/notifications from ScoopWhoop.
   2. In case you need to touch base, please use the "Contact Us" link provided on scoopwhoop.com or contact the Data Protection Officer, appointed hereinbelow.However, please note that your right to review, update, correct, and delete your personal information may be limited, subject to the law of your jurisdiction:
      1. if your requests are abusive or unreasonably excessive,
      2. where the rights or safety of another person or persons would be encroached upon,
      3. if the information or material you request relates to/conflicts with any existing or anticipated legal proceedings and/or negotiations between you and us and/or any third party, or
      4. if in contradiction to our records retention policies and/or any other applicable law, including any statutory retention requirements.
   3. Please note if you delete your User Contributions from our websites, copies of your User Contributions may remain viewable in cached and archived pages, or might have been copied or stored by other users of our websites.
2. **INFORMATION SECURITY**

Please note that appropriate physical, electronic and managerial procedures, in compliance with accepted industry standards, have been implemented to safeguard and help prevent unauthorized access to your information and to maintain data security. These safeguards are subjected to the sensitivity of information that is collected, processed and stored and the current state of technology.

We assume no liability or responsibility for disclosure of your information due to errors in transmission, unauthorized third-party access, or other causes beyond our control. You play an important role in keeping your personal information secure. You should not share your personal information with anyone. If we receive instructions using your personal information, we will reckon that the instructions have been authorized by you.

1. **JOB APPLICANTS**

If your information is submitted to us through the email id - jobs@scoopwhoop.com for securing a position with us, the information will be used to consider your application. We may choose to retain the information provided for any period of time and share the same with third parties for the purpose of evaluating your candidacy.

1. **AMENDMENT TO THIS PRIVACY POLICY**

We reserve the right, at our sole discretion, to change this Privacy Policy on a going-forward basis at any time. Please check this Privacy Policy periodically for changes. Modified Privacy Policy becomes effective upon its publication on the Website. By continuing to use our services, you agree to be bound by the updated, amended, or modified Privacy Policy. If you do not agree to be bound by the modified Privacy Policy, you must immediately cease your use of our services. Disputes arising under this Privacy Policy will be resolved in accordance with the version of this Privacy Policy that was in effect at the time the dispute arose.

1. **GRIEVANCE OFFICER**

Should you have questions about this Privacy Policy or ScoopWhoop's information collection, use, processing and disclosure practices, you may contact, the appointed Grievance Officer, details provided hereinbelow:

**Name:** Mr Piyush Yadav  
**Email:** grievance-officer@scoopwhoop.com  
**Address:** C5, Green Avenue Street, Mall Road, Near Fortis Hospital, Vasant Kunj, Delhi 110070.

We request you to please provide the following information in your complaint:-

* 1. Clear statement as to whether the information is personal information or sensitive personal information;
  2. Identification of the information provided by you;
  3. A statement, under penalty of perjury, that the information in the notice is accurate, and that the information being complained about belongs to you;
  4. A statement that you have a good-faith belief that the information has been processed incorrectly or disclosed without authorization, as the case may be;
  5. Your address, telephone number or e-mail address;
  6. You may also contact us in case you have any questions / suggestions about the Privacy Policy using the contact information mentioned above.

Any communication pursuant to this Clause which is not marked to the designated individual mentioned hereinabove shall not be treated as a valid and binding communication for the purpose of this Privacy Policy.

SSH Communication Security

**Data Privacy Policy**

SSH Communications Security is committed to preserving your right to privacy and we take all appropriate steps to protect your information both online and offline. For terms and conditions of use of SSH.COM Website, please see the [**Website Terms of Use**](https://www.ssh.com/legal/terms_of_use_ssh_website).

SSH Communications Security Corporation is the controller for any personally identifiable information we obtain and store for the purposes of EU GDPR. Our representative in the European Union is General Counsel, SSH Communications Security Corporation, Karvaamokuja 2 B, 00380 Helsinki, Finland. Depending on your jurisdiction, you may have additional rights to obtain or control information we have about you.

In case you have any questions in relation to this data privacy policy or use of personal information by SSH, please contact us via email at dataprotection@ssh.com.

**Data processing**

SSH processes personal data of its customers, potential customers, marketing contacts and other persons who have showed interest towards SSH products and services. Processing activities are conducted for sales and marketing purposes, invoicing, payments and transactions, analytics, customer relationship management, development of business operation and other comparable business purposes. The processing is necessary to conduct legitimate business operations based on legitimate interest.

SSH also processes personal data of its customers to enable commercial transactions in the online store based on legitimate commercial interest.

As an employer, SSH also processes personal details of its employees, consultants, contractors, former employees and job applicants. The processing is necessary for recruitment, human resources, employment and administrative purposes to manage employee and job applicant relationships effectively and appropriately, and to fulfil employer duties accordingly to appropriate legislation at a time. The processing activities can be based on contractual responsibilities arising from applicable employment contracts, such as salary payment and sick pay, legal obligations imposed by employment law and other relevant legislation, including taxation purposes and occupational health care obligations, and legitimate interest, including business compliance, reporting duties and administrative purposes. SSH may also rely on consent for specific processing purposes, such as recruitment and background checks.

**Personal data processed by us**

The personal information SSH may process related to its customers, potential customers and marketing contacts may include the following data:

* contact information (name, home/correspondence address, email address, phone number;
* position/title, company name;
* IP address, log data;
* invoicing/payment details and bank account number.

Personal information SSH processes of its employees, consultants, contractors and former employees may depend on position within SSH and the requirements of applicable laws, but may include the following data:

* contact information (name, home/correspondence address, email address, phone number, emergency contact information);
* other personal information (date of birth, social security number, national identification number, nationality, preferred language, passport number);
* job applications, references, resumes;
* employment contracts and amendments;
* visas, immigration data;
* bank account number and payroll information
* holiday, sickness and absence data;
* vehicle license plate number;
* health information related to occupational health care;
* education details, employment details, employment history;
* photos, videos;
* recommendation letters, employment certificates, termination letters.

Personal information SSH processes of job applicants may include the following data:

* contact information (name, home/correspondence address, email address, phone number);
* other personal information (date of birth, nationality, preferred language);
* job application, references, resumes;
* previous working experience.

**Sources of personal data**

Most of the personal data processed by SSH is collected directly from the data subjects, including information entered into the forms of the Website. SSH also processes personal data in connection with contractual relationships. Personal data may also be collected indirectly, for example from marketing lists and third-party providers.

**Lawful basis for processing**

We process personal information based on the most appropriate lawful basis for processing depending on the specific processing purpose. We never process any personal data without a valid lawful basis for processing.

Lawful bases for processing:

* explicit, specific and unambiguous consent
* contractual obligation
* legal obligation
* legitimate interest
* vital interest
* public interest

**Disclosure of data**

We treat your personal information confidentially and only share it when there is a business reason to do so, including improving our marketing. This includes sharing information within the SSH group and with the channel partners and other organizations related to our business. We do not sell or distribute any personal information for third-party marketing.

**Recruitment data**

We collect and store personal data you submit via the recruitment system in the course of the recruitment process. The recruitment purposes include identifying and evaluating candidates for open positions as well as for possible future roles. SSH may also process your personal data to ensure compliance with applicable legal requirements. For more information about privacy and use of personal data in our recruitment, please refer to the [**Recruitment Privacy Policy**](https://assets.ctfassets.net/0lvk5dbamxpi/5vMV8kMIfjwL1ppUn3J4cH/f301af6261988c73a6f69f038cf0b875/Recruitment_privacy_policy_2018.pdf).

**Profiling and automated decision-making**

SSH does not process personal data for profiling or automated decision-making.

**IP addresses and log data**

We collect and use visitor IP addresses and log data for cybersecurity and analytics purposes. We remove or anonymize personally identifiable IP address information when it is no longer relevant for possible security investigations.

**Unsubscribing from marketing emails**

All marketing emails include opt out possibility. If at any time you wish to no longer receive marketing emails from SSH Communications Security, you may opt out of future electronic marketing communications by locating the most recent email communication received from SSH and clicking the UNSUBSCRIBE and/or EMAIL PREFERENCE links located in the footer of the email. If you have previously unsubscribed from email communications before and would like to re-subscribe to specific SSH email subscriptions, please email webteam@ssh.com.

**Data retention**

SSH retains and stores data for business and compliance reasons. With exception of storage, processing activities will cease immediately when there is no longer lawful basis for processing. All data is destructed within applicable time limits in accordance with applicable laws and regulations. SSH respects the principle of data minimization and all data is limited to what is necessary for the purposes of processing. If you wish to know more about our specific data retention periods or the criteria to determine the periods, please contact us at dataprotection@ssh.com.

**Security of processing**

SSH has adopted high standards of technical and organizational measures to ensure security in both electronical and physical data processing. Data retained in electronic form is secured with strong technical safety measures, including appropriate firewalls and encryption. Physically processed data is kept safely in storages with electronic locks. Your personal information will be kept confidential, and only limited people with effective non-disclosure agreements will have access to your personal data.

Absolute security can never be guaranteed, but SSH is committed to ensure the highest security measures available at a time. If a data breach occurs within SSH Group, it will be notified according to the GDPR rules and time limits.

**International transfers of personal data**

SSH may sometimes need to transfer personal information outside the EU. International data transfers may typically take place to USA and Hong Kong due to the geographical locations of SSH subsidiaries. When international data transfers are required, they are made in accordance with the appropriate safeguards defined in the GDPR.

**Anonymous data collection**

In general, you can visit the Website without providing us with any personal information about yourself or your organization. However, we do collect statistical information about how users behave on this Website to improve the Website, understand our visitor demographics, and to provide more relevant content to our visitors. Anonymous data collection is also done by third-party service providers. In most cases, our cookies and statistical data we collect are pseudonymous and we have no legal means to associate them with an individual person. In such cases, they are not personally identifiable information. For more information about the use of SSH Website and cookies, please see the [**Website Terms of Use**](https://www.ssh.com/legal/terms_of_use_ssh_website).

**Rights of the data subjects**

SSH respects the principles of fair and transparent data processing and makes sure that all applicable rights are available to data subjects.

Depending on your jurisdiction, you may have the following personal privacy rights available to you:

* right to be informed of collection and use of your personal data
* right to access your personal data and any supplementary information
* right to rectification of your personal data if it is inaccurate or incomplete
* right to data portability when you want to transfer data to different service or IT-environment
* right to erasure when there is no purpose to continue processing or if data has been processed unlawfully
* right to withdraw consent for processing at anytime
* right to restrict processing when data is inaccurate, processing is unlawful, or when processing is based on legitimate interest and there are no overriding legitimate grounds to continue processing or the grounds are pending by the controller
* right to object direct marketing, including profiling, or processing for statistics, or processing based on legitimate or public interest
* right to lodge a complaint with the supervisory authority if you consider that processing of your data infringes the GDPR

**Obtaining or removing your personal information**

If you wish and your jurisdiction gives you the right to obtain a copy of your personal information or to remove it, you can email us at dataprotection@ssh.com.

If you have a right to obtain a copy of your personal data, we will provide you with the following information:

* confirmation that SSH is processing your personal data
* free copy of the personal data
* purposes for processing
* categories of the personal data
* sources of the personal data
* data retention periods, or explanation how the length will be determined
* recipients of the personal data
* transfers to third countries
* existence of additional rights
* information on the right to complain to the supervisory authority in case of a personal privacy violation

We will comply with data access and/or erasure requests within one (1) month from the date of the request. SSH has right to decline any unreasonable, repetitive or excessive requests according to the GDPR.

**Obtaining or removing your data from the SSH.COM online shop**

If you wish to access or remove your information from the [**SSH.COM online shop**](https://shop.ssh.com/), you have the possibility to sign up to your account and delete your personal information.

**Right to change these terms**

SSH Communications Security reserves the right to change, modify, or update these terms at any time without notice. These terms were last modified on May 25, 2018.

Mozilla

**At Mozilla, we believe that privacy is fundamental to a healthy internet.**

That’s why we build Firefox, and all our products, to give you greater control over the information you share online and the information you share with us. We strive to collect only what we need to improve Firefox for everyone.

In this Privacy Notice, we explain what data Firefox shares and point you to settings to share even less. We also adhere to the practices outlined in the Mozilla [privacy policy](https://www.mozilla.org/privacy/) for how we receive, handle and share information we collect from Firefox.

**Firefox by default shares data to:**

**Improve performance and stability for users everywhere**

* **Interaction data**: Firefox sends data about your interactions with Firefox to us (such as number of open tabs and windows; number of webpages visited; number and type of installed Firefox Add-ons; and session length) and Firefox features offered by Mozilla or our partners (such as interaction with Firefox search features and search partner referrals).
* **Technical data**: Firefox sends data about your Firefox version and language; device operating system and hardware configuration; memory, basic information about crashes and errors; outcome of automated processes like updates, safebrowsing, and activation to us. When Firefox sends data to us, your IP address is temporarily collected as part of our server logs.

Read the telemetry documentation for [Desktop](https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/telemetry/index.html), [Android](https://firefox-source-docs.mozilla.org/mobile/android/index.html), or [iOS](https://github.com/mozilla-mobile/firefox-ios/wiki/Telemetry) or learn how to opt-out of this data collection on [Desktop](https://support.mozilla.org/en-US/kb/share-data-mozilla-help-improve-firefox?redirectlocale=en-US&redirectslug=send-performance-data-improve-firefox) and [Mobile](https://support.mozilla.org/en-US/kb/send-usage-data-firefox-mobile-browsers).

**Set a default search provider**

* **Location data**: When you first use Firefox, it uses your IP address to set your default search provider based on your country. [Learn more](https://support.mozilla.org/kb/change-your-default-search-settings-firefox).

**Suggest relevant content**

Firefox displays content, such as “Snippets” (messages from Mozilla), Add-on Recommendations, Top Sites (websites suggested by Mozilla for first-time Firefox users), and Pocket Recommendations (which is part of the Mozilla family).

* **Location data**: Firefox uses your IP address to suggest relevant content based on your country and state.
* **Technical & Interaction data**: Firefox sends us data such as the position, size and placement of content we suggest, as well as basic data about your interactions with Firefox’s suggested content. This includes the number of times suggested content is displayed or clicked.
* **Webpage data for Snippets**: When you choose to click on a Snippet link, we may receive data about the link you followed. This information is not associated with any other information about you. [Learn more](https://abouthome-snippets-service.readthedocs.io/en/latest/data_collection.html).
* **Webpage, Language, and Location data for Pocket Recommendations**: We recommend content to you based on your browsing history, language, and country location. The process of deciding which stories you should see based on your browsing history happens locally in your copy of Firefox, and neither Mozilla nor Pocket receives a copy of your browsing history. To help you see relevant Pocket Recommendations based on your location, Firefox shares your language and country location with Pocket.

Mozilla and Pocket receive aggregated data about the recommendations you see and click. We also share aggregated data about the sponsored content you see and click with our third-party ad platform Adzerk so advertisers can see how many people click on their articles. This aggregated data does not identify you personally.

* **Location data and Interaction data for Top Sites**: When you click the Amazon.com Top Site tile on New Tab, we share your country and the time you clicked with Amazon and AdMarketplace (a third-party referral platform) to verify you navigated to Amazon. Firefox does not share your IP address or any other information that could be used to identify you with either Amazon or AdMarketplace.
* **Add-on and Feature Recommendations**: We recommend Add-ons in two places: the Manage Your Extensions Page (about:addons) and the Awesome Bar, where you search or type in URLs. We may also recommend Firefox Features in the Awesome Bar. We base the recommendations in about:addons on a cookie. We base the recommendations in the Awesome Bar on your interaction with Firefox. Mozilla does not receive your browser history. The process happens locally in your own computer’s copy of Firefox. Learn More about [Awesome Bar recommendations](https://support.mozilla.org/kb/extension-recommendations) or [Extensions Page recommendations](https://support.mozilla.org/kb/personalized-extension-recommendations).

**Improve security for users everywhere**

**Webpage data to DNS Resolver service**: For some Firefox users in the United States, Firefox routes DNS requests to a resolver service that has agreed to Mozilla’s [strict privacy standards for resolvers](https://wiki.mozilla.org/Security/DOH-resolver-policy). This provides added protection from privacy leaks to local networks and also from certain DNS security attacks. System logs of your DNS requests are deleted from the service within 24 hours and are only used for the purpose of DNS resolution. [Learn more](https://support.mozilla.org/kb/firefox-dns-over-https#w_switching-providers) or see our default DNS resolver service providers below:

* [**Cloudflare**](https://developers.cloudflare.com/1.1.1.1/privacy/firefox/)
* [**NextDNS**](https://nextdns.io/privacy)
* [**Comcast**](https://www.xfinity.com/privacy/policy/dns)

**Technical data for updates**: Desktop versions of Firefox check for browser updates by persistently connecting to Mozilla servers. Your Firefox version, language, and device operating system are used to apply the correct updates. Mobile versions of Firefox may connect to another service if you used one to download and install Firefox. [Learn more](https://support.mozilla.org/kb/how-stop-firefox-automatically-making-connections#w_auto-update-checking).

**Technical data for add-ons blocklist**: Firefox for Desktop and Android periodically connect to Mozilla to protect you and others from malicious add-ons. Your Firefox version and language, device operating system, and list of installed add-ons are needed to apply and update the add-ons blocklist. [Learn more](https://support.mozilla.org/kb/how-stop-firefox-making-automatic-connections).

**Webpage and technical data to Google’s SafeBrowsing service**: To help protect you from malicious downloads, Firefox sends basic information about unrecognized downloads to Google's SafeBrowsing Service, including the filename and the URL it was downloaded from.[Learn more](https://support.mozilla.org/kb/how-does-phishing-and-malware-protection-work) or read [Google’s Privacy Policy](https://www.google.com/policies/privacy/). Opting out prevents Firefox from warning you of potentially illegitimate or malicious websites or downloaded files.

**Webpage and technical data to Certificate Authorities**: When you visit a secure website (usually identified with a URL starting with "HTTPS"), Firefox validates the website's [certificate](https://support.mozilla.org/kb/secure-website-certificate). This may involve Firefox sending certain information about the website to the Certificate Authority identified by that website. Opting out increases the risk of your private information being intercepted. [Learn more](https://support.mozilla.org/kb/advanced-settings-browsing-network-updates-encryption#w_certificates-tab).

**Crash reports**

By default on desktop versions of Firefox, we will ask you to share a report with more detailed information about crashes with Mozilla, but you always have the choice to decline.

* **Sensitive data**: Crash reports include a ‘dump file’ of Firefox’s memory contents at the time of the crash, which may contain data that identifies you or is otherwise sensitive to you.
* **Webpage data**: Crash reports include the active URL at time of crash.
* **Technical data**: Crash reports include data on why Firefox crashed and the state of device memory and execution during the crash.

Read the full documentation [here](https://firefox-source-docs.mozilla.org/toolkit/crashreporter/crashreporter/index.html).

**Measure and support our marketing**

* **Campaign and Referral Data**: This helps Mozilla understand the effectiveness of our marketing campaigns.

*On Desktop*: Firefox by default sends Mozilla HTTP data that may be included with Firefox’s installer. This enables us to determine the website domain or advertising campaign (if any) that referred you to our download page. Read the [documentation](https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/telemetry/data/environment.html#attribution) or [opt-out](https://support.mozilla.org/kb/desktop-privacy) before installation.

*On Android*: Firefox by default sends mobile campaign data to Adjust, our analytics vendor, which has its own [privacy policy](https://www.adjust.com/terms/privacy-policy/). Mobile campaign data includes a Google advertising ID, IP address, timestamp, country, language/locale, operating system, and app version. Read the [documentation](https://firefox-source-docs.mozilla.org/mobile/android/adjust.html).

* **Technical & Interaction Data**:

*On iOS and Android*: Firefox by default sends data about what features you use in Firefox to Leanplum, our mobile marketing vendor, which has its own [privacy policy](https://www.leanplum.com/privacy/). This data allows us to test different features and experiences, as well as provide customized messages and recommendations for improving your experience with Firefox.

Read the documentation for [iOS](https://github.com/mozilla-mobile/firefox-ios/blob/master/Docs/MMA.md) or [Android](https://firefox-source-docs.mozilla.org/mobile/android/mma.html), or learn how to [disable this feature](https://support.mozilla.org/kb/send-anonymous-usage-data-firefox-mobile-devices).

**If you use these features, Firefox will share data to provide you functionality and help us improve our products and services:**

**Search**

You can perform searches directly from several places in Firefox, including the Awesome Bar, Search Bar, or on a New Tab. *Mozilla does not receive your search queries.* We do receive data about how you engage with search in Firefox and the number of searches you request from our search partners. Query data is sent to your search provider, which has its own privacy policy. Links to our default search providers are:

* [**Google**](https://policies.google.com/privacy)
* [**Microsoft (Bing)**](https://privacy.microsoft.com/privacystatement)
* [**Yandex**](https://yandex.ru/legal/confidential/)

**Search Suggestions**: Firefox by default sends search queries to your search provider to help you discover common phrases other people have searched for and improve your search experience. These data will not be sent if your selected search provider does not support search suggestions.

[Learn more](https://support.mozilla.org/kb/use-popular-search-suggestions-firefox-search-bar), including how to disable this feature.

**Firefox Accounts & Join Firefox**

* **Registration data**: Mozilla receives your email address and a hash of your password when you create a Firefox Account or sign-up to Join Firefox. You can choose to include a display name or profile image. Your email address is sent to our email vendor, SalesForce Marketing Cloud, which has its own [privacy policy](https://www.marketingcloud.com/privacy-policy/website-privacy-statement/).
* **Location data**: For security purposes, we store the IP addresses used to access your Firefox Account in order to approximate your city and country. We use this data to send you email alerts if we detect suspicious activity, such as account logins from other locations.
* **Interaction data**: We receive data such as your visits to the Firefox Accounts website, dashboards and menu preferences, what products and services you use in connection with your Firefox Account, and your interactions with our emails and SMS messages. We use this to understand your use of our products and services and to send you more useful Firefox Account Tips and in-product messages.
* **Technical data**: To display which devices are synced to your Firefox Account and for security functionality, we store your device operating system, browser and version, timestamp, locale, and the same information for devices connected to your account. If you use your Firefox Account to log into other websites or services (such as AMO or Pocket), we receive the timestamp of those log-ins.

Read the full documentation or learn more, including how to manage your Firefox Account data or our data practices for [websites and email](https://www.mozilla.org/privacy/websites/). You can also read the privacy notices for our Firefox Account connected services, which are:

* [Firefox Lockwise](https://support.mozilla.org/kb/firefox-lockwise-and-privacy)
* [Firefox Monitor](https://www.mozilla.org/privacy/firefox-monitor)
* [Firefox Notes](https://addons.mozilla.org/firefox/addon/notes-by-firefox/)
* [Firefox Send](http://send.firefox.com/legal)
* [Firefox Sync](https://www.mozilla.org/privacy/firefox/#sync)

**Sync**

* **Synced data**: If you enable Sync, Mozilla receives the information that you sync across devices in encrypted form. This may include Firefox tabs, add-ons, passwords, payment autofill information, bookmarks, history, and preferences. Deleting your Firefox Account will delete related Firefox Sync content. You can also read the [documentation](https://moz-services-docs.readthedocs.io/en/latest/sync/).
* **Technical and Interaction data**: If you enable sync, Firefox will periodically send basic information using Telemetry about the most recent attempt to sync your data, such as when it took place, whether it succeeded or failed, and what type of device is attempting to sync. You can also read the [documentation](https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/telemetry/data/sync-ping.html).

[Learn more](https://support.mozilla.org/kb/how-do-i-set-sync-my-computer), including how to enable or disable sync.

**Location**

* **Location data to Google's geolocation service**: Firefox always asks before determining and sharing your location with a requesting website (for example, if a map website needs your location to provide directions). To determine location, Firefox may use your operating system’s geolocation features, Wi-fi networks, cell phone towers, or IP address, and may send this data to Google's geolocation service, which has its own [privacy policy](https://www.google.com/privacy/lsf.html).

[Learn more](https://www.mozilla.org/firefox/geolocation/).

**Website notifications**

* **Connection data**: If you allow a website to send you notifications, Firefox connects with Mozilla and uses your IP address to relay the message. Mozilla cannot access the content of messages.
* **Interaction data**: We receive aggregate data such as the number of Firefox subscriptions and unsubscriptions to website notifications, number of messages sent, timestamps, and senders (which may include specific website providers).

Read the [full documentation](https://mozilla-push-service.readthedocs.io/en/latest/) or [learn more](https://support.mozilla.org/kb/push-notifications-firefox), including how to revoke website notifications.

**Add-ons**

**Footnote**

This privacy notice is for the most recent general release version of Firefox distributed by Mozilla. If you obtain Firefox elsewhere, or are running an older version, your copy of Firefox may contain different privacy characteristics.

Mozilla’s pre-release versions of Firefox (which are distributed through channels such as Nightly, Beta, Developer Edition and TestFlight) are development platforms frequently updated with experimental features and studies.  In addition to the data collection described in this Privacy Notice, these versions by default may send certain types of web activity and crash data to Mozilla and in some cases to our partners. Any data collection or sharing adheres to our [Firefox data collection policy](https://wiki.mozilla.org/Firefox/Data_Collection) and we will always be transparent and provide you with controls

**Thunderbird Collects Data To:**

**Improve Performance and Stability For Our Users**

Thunderbird collects telemetry data by default to help improve the performance and stability of Thunderbird. There are two types of telemetry data: interaction data and technical data.

**Interaction data**: Thunderbird receives data about your interactions with the application, such as whether calendars and filters are being used, and how many email accounts a user has.

**Technical data**: Thunderbird also receives basic information about your device and application version, including, hardware configuration, device operating system, and language preference. When Thunderbird sends technical data to us, your IP address is temporarily collected as part of our server logs.

Read the telemetry documentation and learn how to opt-out of this data collection [here](https://support.mozilla.org/kb/thunderbird-telemetry).

**Set-Up and Configure Your Email**

Thunderbird collects your email domain and other technical data to set-up and configure your email account. Other information, like your name, your email messages, and your account’s address book are stored locally on your computer and never sent to us. Learn more [here](https://support.mozilla.org/kb/automatic-account-configuration).

**Email domain**: Thunderbird receives your email address domain. Your full email address is never processed or stored on our servers (unless you choose to share it when you send a crash report).

**Technical data**: Thunderbird also receives information about the application’s version and device operating system. When Thunderbird sends technical data to us, your IP address is temporarily collected as part of our server logs.

**Review Crash Reports**

If Thunderbird crashes, we will ask you to share a report with more detailed information about the crash, but you always have the choice to decline. Thunderbird uses the information in the crash report to diagnose and correct the problem that caused the crash.

**Sensitive data**: Crash reports include a “dump file” of Thunderbird’s memory contents at the time of the crash, which may contain data that identifies you or is otherwise sensitive to you.

**Webpage data**: Crash reports include any active URLs at time of crash.

**Add-on data**: Crash reports include a list of all add-ons that you were using at the time of the crash, and the time since: the start-up of the program, the last crash, and the last install.

**Technical data**: Crash reports include data on why Thunderbird crashed and the state of device memory and execution during the crash. When Thunderbird sends technical data to us, your IP address is temporarily collected as part of our server logs.

**Email address**: If you choose, crash reports include your email address.

Read the full documentation [here](https://support.mozilla.org/kb/mozilla-crash-reporter-tb).

**Improve Security for Our Users Everywhere**

**Technical data for updates**: To ensure you have the most up-to-date version of the product, Thunderbird checks for updates by periodically connecting to Thunderbird’s servers. Your application version, language, and device operating system are used to apply the correct updates. [Learn more](https://support.mozilla.org/kb/thunderbird-makes-unrequested-connections#w_auto-update-checking).

**Technical data for add-ons blocklist**: To help to protect you from any malicious add-ons, Thunderbird periodically checks for blocklisted add-ons. Your Thunderbird version and language, device operating system, and list of installed add-ons are needed to apply and update the add-ons blocklist. [Learn more](https://support.mozilla.org/kb/thunderbird-makes-unrequested-connections#w_extension-blocklist-updating).

**Install and Update Add-Ons**

You can install add-ons from addons.thunderbird.net or from the Thunderbird Add-ons Manager, which is accessible by clicking on Tools > Add-ons. To keep your installed add-ons up to date—like add-on descriptions, download counts, and ratings—the Thunderbird application periodically connects to our servers to install any updates.

**Search queries**: If you enter keywords into the search field for the Add-ons Manager, those keywords will be sent to Thunderbird to perform the search.

**Interaction data**: We receive aggregate data about visits to the Thunderbird website and the Add-ons Manager in Thunderbird, as well as interactions with content on those pages. Read about data practices on [Mozilla websites](https://www.mozilla.org/privacy/websites/).

**Technical data for updates**: Thunderbird periodically connects to our server to install updates to add-ons. Your installed add-ons, application version, language, and device operating system are used to apply the correct updates. When Thunderbird sends technical data to us, your IP address is temporarily collected as part of our server logs.

**Thunderbird May Disclose Information To:**

**Mozilla Affiliates**: Thunderbird is a project of MZLA Technologies Corporation, a subsidiary of Mozilla Foundation and as such, shares some of the same infrastructure. This means that, from time to time, your data (e.g., crash reports, and technical and interaction data) may be disclosed to Mozilla Corporation and Mozilla Foundation. If so, it will be maintained in accordance with the commitments we make in this Privacy Notice.

**DNS servers, Standard Autoconfiguration URIs, and Mozilla's Configuration Database**: To simplify the email set-up process, Thunderbird tries to determine the correct settings for your account by contacting Mozilla’s configuration database as well as external servers. These include DNS servers and standard autoconfiguration URIs. During this process, your email domain may be sent to Mozilla's configuration database, and your email address may be disclosed to your network administrators.

**Amazon Web Services**: Thunderbird uses Amazon Web Services (AWS) to host its servers and as a content delivery network. Your device’s IP address is collected as part of AWS’s server logs.

**Gandi.net**: Thunderbird has partnered with Gandi.net to allow you to create a new email address through Thunderbird. If you choose to use this feature, your email address search terms are sent to Gandi.net to return available addresses. In addition, your country location is also shared with Gandi.net to provide the correct prices. You can learn more about Gandi.net’s data practices by reading their [Privacy Policy](https://contract.gandi.net/v5/contracts/14420/Privacy_Policy_US_2.0_en.pdf).

Gandi.net

Gandi Privacy Policy

Last Update September 1, 2016 - Version 2.0

Thank You for visiting our Privacy Policy. This policy applies to information collected on Our bêta version https://beta.gandi.net and all

affiliated websites that link to this Policy (collectively referred to herein as the "Sites", “Gandi”, "We" or "Us").

Gandi is strongly committed to protecting the privacy of those who entrust Us with their personal information. Visitors to Our Sites, Our

customers and all those who do business with Us trust and expect that We will protect their Personal Information. We want You to know

that We take the privacy, security and confidentiality of Your information, including any personally identifiable information ("Personal

Information" or "PII") extremely seriously. Accordingly, We take all commercially practicable and available precautions to ensure the

security and confidentiality of Personal Information.

We also want You to know what information we collect, why and how we will treat it once collected. Finally, We want You to be able to

have control over Your Personal Information so that if You need to update or to correct Your information or want to opt-out of receiving

certain communications, You can do that easily. Please read it carefully.

CONSENT:

BY ACCESSING THE SITES AND/OR CREATING A GANDI ACCOUNT OR ALLOWING SOMEONE TO USE THE SITES ON YOUR

BEHALF, YOU ARE CONSENTING TO THE COLLECTION, USE, DISCLOSURE, TRANSFER AND STORAGE OF PERSONAL

AND NON-PERSONAL INFORMATION OR OTHER INFORMATION RECEIVED BY US AS A RESULT OF SUCH USE IN

ACCORDANCE WITH THIS PRIVACY POLICY.

Your California Privacy Rights, Our Contact Info & Requests for Information

It is vitally important for You to keep Your Personal Information accurate, current and complete at all times, as well as for You to be able

to reach Us should You have any questions or concerns regarding this Privacy Policy. If We are unable to address Your issue

immediately, We will respond as soon as possible. Pursuant to Section 1798.83 of the California Civil Code, residents of California can

obtain certain information about the types of PII that companies with whom they have an established business relationship have shared

with third parties for direct marketing purposes during the preceding calendar year. In particular, that law provides that consumers may

request a copy of the PII that We hold about You. Consumers may also request information regarding the categories of PII that have

been shared with third parties, the names and addresses of those third parties and examples of the types of services or products

marketed by those third parties. To request either a copy of the PII maintained by Us about You or to request a copy of the information

disclosure provided by Us during the preceding calendar year pursuant to Section 1798.83 of the California Civil Code, please contact

Us via email at: us-privacy@gandi.net, or by writing Us at the below address. Please allow 30 days for a response.

Gandi US, Inc.

Attention: Privacy

121 2nd St. Ste 500

San Francisco, CA 94105

Phone: (410) 429-7400

Fax: (410) 429-7400

What Information Is Collected?

1. Personal Information

We may collect Personal Information from users of the Sites in several instances. Some examples are as follows:

• We may collect Your name, billing address, shipping address, email address, telephone number. This information is used to provide

the products and services that You have ordered or requested and order confirmations (or other transactional information) and/or to

provide customer service.

• We may collect information regarding the domain names that You own or have owned. This information is used to provide the

services that You have requested and to suggest additional services that We believe You may be interested in via Domain Suggest

for example.

• We may collect Your name, email address, mailing address, zip code, and date of birth if You create a User Account and a Personal

Organization and Legal Contacts. This information will be used to help You keep track of Your orders, to keep You updated about

special offers, updates related to the Sites and any of the Gandi Contracts or other agreements which are applicable to the products

or services You have purchased or to which You have subscribed, and to facilitate checkout during purchases.

• We may collect Your IP address, Your status (natural person, legal person, association, public organization,...), the language of Your

web browser and the keyword queried to suggest You additional domain names during the purchase, to propose alternatives if the

domain queried is no longer available.

• We may collect Your email address if You sign up to receive promotional emails from Us. This information may be used to contact

You about sales, special offers and new features available through the Sites.

• We may collect Your name, telephone number, mailing address, zip code, and email address if You contact Us with a question or

request customer support from Us. This information may be used so that we can respond to Your question or contact You regarding

Your request.

1/5

• We may collect Your name, email address, and other contact information if You participate in a promotion (e.g., contest,

sweepstakes) that We sponsor. This information will be used to fulfill the terms of the promotion and to contact You regarding

promotional and special offers, sales, and new features available through the Sites. It will also be subject to the terms accompanying

such promotion.

• We may collect Your name, age, zip code, purchasing habits, email address and/or mailing address if You choose to participate in

one of our on-line surveys. This information will be used to help provide Us with relevant information about Our customers.

• We may collect and maintain more extensive PII (including driver’s license numbers, passport numbers, identity card, etc.) if You are

purchasing a Gandi SSL Certificate, as We are required to review proof of identification and related documentation to verify Your

identity in order to issue You the Gandi SSL Certificate for which You are applying.

• We may collect and maintain more extensive PII (including driver’s license numbers, passport numbers, etc.) if You are purchasing

some extensions (domain names) which require supporting documentation.

Of course, You can update Your information or change Your preferences regarding receiving announcements and other information

from Us at any time by accessing Your account via the Sites. (For more information, see below section entitled How Can I Access,

Correct and Update My Personal Information?). The above section provides examples of the Personal Information that We may collect

through the Sites (including the bêta version of Our Sites) and the manners in which We may use such Personal Information. If You do

not want Us to collect Your Personal Information, please do not provide it to Us.

2. Non-Personal Information

You do not need to create an account with Us to use the Sites. When You use the Sites, including by browsing our products and

services and/or contacting Us with inquiries, We collect certain non-identifiable information ("Non-Personal Information"). The NonPersonal Information we collect includes, without limitation, Internet Protocol (IP) addresses, Internet browser information, other

characteristics of Your device and software, domain names of Your Internet Service Provider (ISP), Your approximate geographic

location, a record of Your usage of our Sites, the time of Your usage and aggregated Personal Information that cannot be used to

specifically identify You. Such information, which is collected passively using various technologies, cannot, in and of itself, be used to

specifically identify You. This information is used to analyze and to improve the Sites (including to help diagnose and prevent problems

with Our servers or Our products or services), to administer Our Site and to provide Our customers with the best experience using Our

Site. We also may receive certain Non-Personal Information (including, without limitation, of the types set forth above) from various

third parties. The Non-Personal Information We receive from third parties may be combined with the information We collect as specified

herein, including Personal Information. If Non-Personal Information is combined with Personal Information, it may be viewed as

Personal Information. However, where the data remains non-personally identifiable, it will still be viewed as Non-Personal Information.

We provide additional information on Our Non-Personal Information collection below:

• Cookies and Other Session Identifiers:

Like many sites, We utilize a technology called "cookies". A cookie is a piece of information that is placed on Your browser when You

access the Sites. In many cases, the information collected using cookies (and related technologies) are used in non-identifiable ways,

without any reference to Personal Information. For example, We use information We collect about users of the Sites to optimize Our

Sites and to understand traffic and usage patterns. In other cases, We associate the information We collect using cookies and related

technologies with Personal Information. In that case, this Privacy Policy governs how we use that information. Additionally, if the

settings on Your location-aware device allow Us to receive geolocation data or information, We may collect that information

automatically. We also use tracking information to determine which areas Our site users visit based on traffic to those areas. Gandi

does not track what individual users read, but rather how often each page is visited.

Cookies help provide additional functionality to the Sites and help Us to more accurately analyze usage of the Sites. For instance, the

Sites may set a cookie on Your browser that allows You to access the Sites during future visits. We use cookies to monitor and to

maintain information about Your use of the Sites. Cookies are also used to track the identity of the website You visited immediately prior

to visiting the Sites; other than that, We do not track information about Your use of other websites. Cookies are not used on the Sites to

store Your account information as this information is stored securely on a server. When You log in at the Sites with Your username and

password through Your User Account, We will assign You a secure session id. The server then passes Your information to You through

this secure session id. Cookies may be session cookies (i.e., last only for one browser session) or persistent cookies (i.e., continue in

Your browser until they are deleted or expire). Some of the cookies. While they are harmless, they may contain demographic

information and depending on Your browser these cookies may not normally be deleted when Your cookies are deleted. Please check

Your browser to determine where these types of cookies are stored and how they may be deleted.

While we recommend that You leave cookies turned on as they allow You to take advantage of some of the features of the Sites, You

have the ability to control the use and moderation of cookies. However, if You elect not to allow cookies to be placed as provided

herein, You may not be able to use or to enjoy all of the services and features of the Sites. Specifically, You can configure the settings

(i) to receive notifications when You are receiving new cookies, (ii) to disable cookies or (iii) to delete cookies. Please refer to Your Web

browser's help section for information on how to do this.

• Other Websites, Including Mobile Applications and Social Media Platforms:

If You use a social media platform or Your mobile device (or other method of communication) to interact with the Sites, that platform or

application may have a specific privacy statement that governs the use of Personal Information related to it. If You have questions

about the security and privacy settings of Your mobile device, please refer to instructions from Your mobile service provider or the

manufacturer of Your device to learn how to adjust Your settings. We do not control the data collection or privacy practices of any thirdparty platform through which You access the Sites or contact Us. You should review the privacy policy and terms of use of any thirdparty site before using it and review and use available controls and settings on Your device to reflect Your preferences.

2/5

How Can I Access, Correct and Update My Personal Information?

You can access, correct and/or update certain personal information that You have provided by logging into Your User Account with Your

Access Codes.

How Do We Use the Information Collected?

1. Personal Information

We may use Personal Information as necessary and to fulfill Your requests, including in the following ways:

Access and Use: If You provide Personal Information in order to obtain access to or use of the Sites or any functionality thereof, We will

use Your Personal Information to provide You with access to or use of the Sites or functionality and to monitor Your use of the Sites or

specific functionalities.

Internal Business Purposes: We may use Your Personal Information for internal business purposes including, without limitation, to help

Us improve the content and functionality of the Sites, to better understand Our users, to improve the Sites (including their bêta

versions), to protect against, identify or address fraudulent activities, to manage Your account and to provide You with customer service

and to generally manage the Sites and Our business.

Marketing: We may use Your Personal Information to contact You for certain marketing and advertising purposes, including, without

limitation, to inform You about offers, contests or surveys which may be of interest to You and to display content and advertising on or

off the Sites which may be of relevance to You. If You wish to change or update Your Personal Information or to change Your

subscription preferences, You may do so as provided herein.

Specific Reason: If You provide Personal Information for a certain reason, We may use the Personal Information in connection with the

reason for which it was provided. For instance, if You contact Us by email, We will use the Personal Information You provide to answer

Your question or to attempt to resolve Your issue and will respond to the email address from which the contact came.

Aggregated Personal Information: In an ongoing effort to better understand and to serve the users of the Sites, we (either directly or

working in concert with our marketing services providers) may conduct research on our customer demographics, interests and behavior

based on Personal Information and other information that has been provided or received by Us. For example, we may combine

information about visitors to the Sites to determine how best to target our marketing and the products and services that we offer in

certain areas of the country. This research may be compiled and analyzed on an aggregate basis and this aggregate information does

not identify You personally and is classified and treated as Non-Personal Information under this Privacy Policy.

Do We Share Your Information?

We are not in the business of selling Personal Information. We consider this information to be a vital part of Our relationship with You.

We do not share with others, or sell or rent to others, any Personal Information provided to us through the Sites or through Our

Customer Service Department, except with Your consent or as described in this Privacy Policy. Additionally, We seek to receive Your

consent before sharing Your information. However, in some cases, Your permission will be implied from the nature of the service

requested or transaction undertaken. Examples of instances in which we share Your Personal Information are provided below:

Order Fulfillment: If You choose to make a purchase on the Sites (including their bêta version), We may collect from You billing address

and other information related to such purchase, and We may use such collected information in order to fulfill Your purchase. We may

also provide such information, or other Personal Information provided by You, to unaffiliated third parties as necessary to complete Your

purchase (Registries, Iron Mountain,...).

Business Transfers: As with any business, it is possible that as Our business develops, We might sell, assign, buy, transfer or otherwise

acquire or dispose of certain businesses or corporate assets. In the event of such or similar event, Personal Information may be part of

the transferred assets. You acknowledge and agree that any successor to or acquirer of Us will continue to have the right to use Your

Personal Information and other information in accordance with the terms of this Privacy Policy.

Parent, Subsidiaries and Affiliates: We may also share Your Personal Information with our parent company, subsidiaries and/or affiliates

consistent with this Privacy Policy. Our subsidiaries and affiliates will be bound to treat and to maintain any Personal Information in

accordance with this Privacy Policy.

Agents, Consultants and Related Third Parties: As noted above, We, like many businesses, sometimes engage other companies to

perform certain business-related functions on Our behalf so that We can focus on Our core business. Examples of these services

include, but are not limited to, payment processing and authorization, fraud protection and credit risk reduction, product customization,

order fulfillment and shipping, marketing and promotional material distribution, website evaluation, data analysis and, where applicable,

data cleansing.

In connection with services those partners provide for Us, We may provide or otherwise give them access to certain Personal

Information, but We authorize them to use this information only in connection with the services they are retained to perform.

Legal Requirements: We may disclose Your Personal Information if required to do so by law (including, without limitation responding to

a subpoena or request from law enforcement, court or government agency) or in the good faith belief that such action is necessary (i) to

comply with a legal obligation, (ii) to protect or defend Our rights, interests or property or that of other customers or users, (iii) to act in

urgent circumstances to protect the personal safety of users of the Sites or the public, or (iv) to protect against legal liability or potential

fraud, as determined in Our sole discretion.

Other uses: If We intend to use any Personal Information in any manner that is not specified herein, We will inform You of such

anticipated use prior to or at the time at which the Personal Information is collected or We will obtain Your consent subsequent to such

collection but prior to such use. In short, We will honor the choices You make regarding Your Personal Information and will inform You

about any other intended uses of such information.

3/5

2. Non-Personal Information

As noted above, Non-Personal Information does not and cannot be used to personally identify You. We may use such information for

any lawful purpose, including sharing Non-Personal Information with Our marketing partners, advertisers and others from time to time.

Examples of such Non-Personal Information include the number of users who visited the Sites during a specific time period or

purchased a specific product or service through the Sites. This information generally is shared in an aggregated form.

What Steps Are Taken To Keep My Information Secure?

We have implemented information security measures that contain administrative, technical and physical controls that are designed to

reasonably safeguard Personal and Non-Personal Information. Even though We have taken and will continue to take significant steps

to protect this information, no company, including us, can fully eliminate all security risks associated with Personal Information. We use

various security measures, including Secure Socket Layer (SSL) encryption technology, to protect information collected, transferred

and retained. If You elect to set up an account on the Sites, You will be asked to provide an email address and password. You must

provide a valid email address and password in order to create and maintain an account, as well as to access account information. We

recommend You select a password with at least 8 characters and consider adding numbers or special characters to further strengthen

Your password. In order to help protect Your personal information, You should be careful about providing Your password to others and

change it periodically. If You wish to update a password, or if You become aware of any loss, theft or unauthorized use of a password,

please contact us at us-privacy@gandi.net.

Moreover, we strongly recommend You to active Our two-factor auth feature to enhance Your security. Please be aware that We may

store Personal Information or such information may be included in databases owned and maintained by Our affiliates, agents or third

party service providers. We take all commercially reasonable steps to protect the security and confidentiality of all Personal Information

provided via the Sites from loss, misuse, unauthorized access, inadvertent disclosure, alteration and/or destruction. However, no

Internet or email transmission is ever fully secure or error free. In particular, email sent to or from the Sites may not always be secure.

Please keep this in mind when disclosing any Personal Information via the Internet or by email.

We do not and will not, at any time, ask You to provide Your Personal Information in a non-secure or unsolicited email or telephone

communication. Identity theft and the practice currently known as "phishing" are of great concern to us. Safeguarding information to

help protect You from identity theft is one of Our priorities. If You receive such an email, please contact us to bring it to our attention.

For more information about phishing, visit the Federal Trade Commission at http://www.consumer.ftc.gov/articles/0003-phishing.

What Choices Do I Have Regarding my Personal Information?

You have several choices available when it comes to Your Personal Information. We will honor the choices You make regarding Your

Personal Information. If You have created and maintained a User Account, a Personal Organisation and Legal Contacts on the Sites,

You will be able to sign in and update Your accounts information. You may also write to Us at the address provided herein and update

Your contact information or to change Your subscription preferences. In addition, You may:

Limit the Personal Information You Provide: You can use the Sites and limit the Personal Information You provide either by disabling

cookies or by not registering an account with us. If You choose to limit the Personal Information You provide and/or to disable cookies,

You may not be able to use certain functionalities of the Sites. For instance, in order to purchase goods and services on the Sites,

payment and shipping information must necessarily be provided.

Manage Your Subscription Preferences: We may send You information by email if You subscribe via Your User Account. You further

understand that consent is not a condition of purchase and that message and data rates may apply.

Please be aware that even if You opt-out of receiving future promotional communications, You may, if You utilize the eCommerce

features of the Sites, be sent certain transactional communications related to the purchase or shipment of items purchased. Thus, if

You order online, We will send You an email confirming Your order and may need to contact You by phone, email or regular mail if We

have questions about Your order. Additionally, an opt-out will not remove You from messages that We are required to send under

relevant laws or regulations or which derives from domain name service obligations..

Social Media & Other Public Platforms: You may also manage the sharing of certain Personal Information with Us when You connect

with Us through a social media platform or application, such as through Facebook Connect or Twitter. Please refer to the privacy

settings of the social media website or application to determine how You may adjust Your permissions and manage the interactivity

between Us and Your social media platform(s) or application(s). When You post information to public forums, including publicly

viewable social media platforms, that information will become available to all who access such platform pages. PLEASE BE

EXTREMELY CAREFUL WHEN DISCLOSING ANY INFORMATION IN CHAT ROOMS, FORUMS AND OTHER PUBLIC POSTING

AREAS. WE ARE NOT RESPONSIBLE FOR THE USE BY OTHERS OF THE INFORMATION THAT YOU DISCLOSE IN CHAT

ROOMS, FORUMS AND OTHER PUBLIC POSTING AREAS.

Third Party Advertisers: We may use advertisers, third party ad networks, and other advertising companies, to serve advertisements on

Our Sites and on third-party websites. Please be advised that such advertising companies may gather information about Your visit to

Our Sites (such as through cookies, web beacons and other technologies) to enable such advertising companies to market products or

services to You, to monitor which ads have been served to Your browser and which web pages You were viewing when such ads were

delivered. If You would like more information about this practice and to know Your choices please visit:

http://www.networkadvertising.org/managing/opt\_out.asp or http://preferences.truste.com/truste/. PLEASE NOTE THAT THIS POLICY

DOES NOT COVER THE COLLECTION AND USE OF INFORMATION BY SUCH ADVERTISING COMPANIES.

What Happens When I Link To or From Another Website?

The Sites may contain links to other websites not operated or controlled by us (the "Third Party Sites"). The policies and procedures set

forth herein do not apply to any Third Party Sites. The owners and operators of all Third Party Sites are responsible for all Personal

Information and Non-Personal Information provided, collected, maintained, stored or otherwise disclosed on those sites, if any.

4/5

The links on the Sites do not imply that we endorse or have reviewed the Third Party Sites, including their privacy policies, if any. We

strongly encourage contacting those sites directly for information on their privacy policies. If You have accessed the Sites through a link

from certain of our advertising or marketing partners, the Sites may include a frame of the applicable advertising or marketing partner.

Nevertheless, the information You provide to us through these framed Web pages is collected by us, and our use of such information is

governed by this Privacy Policy.

How Do We Respond to Do Not Track Signals?

Please note that our Sites do not support “Do Not Track” browser settings and do not currently participate in any “Do Not Track”

frameworks that would allow us to respond to signals or other mechanisms from You regarding the collection of Your personal or nonpersonally identifiable information.

Is Information Collected From Children?

Protecting the privacy of children is extremely important to us. The Sites are directed toward a general audience and are not directed at

nor intended for use by children. We do not knowingly collect or intend to collect Personal Information from anyone who is under the

age of 13. If You are under the age of 13, You should not provide any Personal Information to us and You should use the Sites only with

the knowledge, permission and involvement of a parent or guardian. We encourage parents and legal guardians to monitor their

children's Internet usage and to help enforce our Privacy Policy by instructing their children never to provide Personal Information

through the Sites. If You have reason to believe that a child under the age of 13 has provided Personal Information to Us, please

contact us and we will endeavor to delete that information from Our databases.

What if I Access the Sites from Outside of the United States?

If You are visiting our Sites from outside the United States, please be aware that You are sending information (including Personal

Information) to the United States where some of Our servers are located. Otherwise, we will hold and process Your Personal

Information and Non-Personal Information in accordance with privacy laws in the United States and this Privacy Policy. Please note

that privacy laws in the United States may not be the same as, and in some cases may be considered less protective than, privacy laws

in other countries. Therefore, by providing Your Personal Information, You consent to the use of Your Personal Information for the uses

identified in this Privacy Policy and to the transfer of Your Personal Information to the United States as indicated above.

How Will I Be Informed About Changes Regarding This Privacy Policy?

The Sites and our business may change from time to time. As a result (and for other business and/or technological reasons), it may be

necessary for us to make changes to this Privacy Policy. We reserve the right to update, change, amend or modify this Privacy Policy

at any time and from time to time without prior notice. Please review this policy periodically, and especially before You provide any

Personal Information. If we make any material changes to this Privacy Policy (as determined by us), we will post a notice on the Sites

notifying users of the changes and providing an opportunity for You to take action relative to those changes prior to their

implementation. In some cases, we also may send a notice via the Gandi Account or by email notifying registered users of upcoming

changes. This Privacy Policy was last updated on the date indicated above. Your continued use of the Sites after any changes or

revisions to this Privacy Policy become effective shall indicate Your agreement with the terms of such revised and then-current Privacy

Policy.

Arbitration; Claims Must be Brought on an Individual Basis

By using this Sites, You agree that any dispute in any manner arising out of or relating in any way to this Privacy Policy, its enforcement

or interpretation, or because of an alleged breach, default, or misrepresentation in connection with any of its provisions, shall be

submitted to binding arbitration with Judicial Arbitration and Mediation Services, Inc. (“JAMS”) in the San Francisco Bay/San Jose,

California area. This arbitration provision is equally binding on claims brought by Gandi as on claims brought by You or others.

Arbitrations will be conducted under the applicable JAMS rules. The parties to arbitration will have all the same claims, legal rights, and

remedies in arbitration that would be available in court. A single neutral arbitrator shall be selected in accordance with the JAMS

Streamlined Arbitration Rules, which shall provide You a reasonable opportunity to participate in the arbitrator selection. The parties to

arbitration will have full right to use legal counsel at their own expense. All costs of arbitration (including arbitrator fees) shall be paid by

Gandi, except only that if You bring the arbitration, you may be charged an initial filing fee that shall not exceed the filing fees that You

would incur for bringing an action in court. You will not be required to pay fees and costs incurred by the opposing parties if You do not

prevail in arbitration.

In arbitration, the parties may conduct reasonable discovery and shall reasonably exchange non-privileged information relevant to the

dispute. The arbitrator’s award shall be in writing and provide a written statement of the essential findings and conclusions. The

arbitrator will not have the power to commit any error of law or legal reasoning, and the award may be vacated or corrected on appeal

to a court of competent jurisdiction for any such error. As an exception to this arbitration provision, no one subject to the provision will

be precluded from seeking remedies in small claims court for disputes or claims within the scope of its jurisdiction. Claims brought on

behalf of or allegedly representing or including other persons or entities, including but not limited to any class, consolidated,

representative, collective, or private attorney general action, shall be a “Class Action”.

Notwithstanding anything else in this Privacy Policy or the JAMS rules, any parties subject to this arbitration provision shall be barred

from bringing or participating in any Class Action for a dispute covered by this arbitration provision. However, if these Class Actions

restrictions are ever deemed illegal, they shall be severed from this arbitration provision. In that event, any Class Action shall be

exempted from this arbitration provision and brought in court. This arbitration provision is subject to the Federal Arbitration Act, and may

be enforced in any court of competent jurisdiction.

-- end of the Privacy Policy --

2016 Gandi US, Inc. All rights reserved.

Wonderhowto

WonderHowTo Privacy Policy

Effective Date: Last revised on Jan 1, 2020

The privacy of registered and unregistered users ("users" or "you") is very important to us. This Privacy Policy intends to describe: what type of information we collect; how we use, share, and guard the information and your choices regarding your use of the WonderHowTo, Gadget Hacks, and Next Reality websites and services (the "Website").

Information We Collect

You may choose to provide us with general or specific information about yourself when using the Website, including a user name and email address. Also, we may collect web surfing data such as your IP address, server log data, cookie information, areas of the Website you have visited, and if you clicked on advertisements. We use different types of technologies to collect this information, including cookies and single-pixel GIFs.

If your browser is configured to accept the cookies, these cookies will be used to recognize your computer when you visit the Website to allow us to provide updates regarding the Website, to learn how you use the Website so that we can develop new services, and to show you advertisements. You can configure your browser to block cookies; however, if you do, the Website may not function properly or at all.

You may also provide us with personal information. For example, if you choose to register at the Website, you will be asked to create a username and provide a valid email address. If you upload, post, or distribute to the Website information, data, text, photos, audio, links, video, images, graphics, or other content or materials of any nature (collectively, "User Submissions"), those User Submissions, along with your username or other information, may be provided to other users. To limit the amount of personal information disclosed you may consider providing a username other than your actual name.

Use and Sharing of Collected Information

We may use non-personally identifiable information collected to improve the quality of the Website; for example, to diagnose problems, assess and maintain security, place ad on webpages receiving more web traffic, and allow you to log in or access your profile information automatically. We may use non-personally identifiable information to determine user demographics, interests, and behavior and may market the Website by sharing non-personally identifiable information with advertisers and other partners. We also may provide your non-personally identifiable information to contractors so that they can perform services for us.

We use information you provide to: (1) handle or respond to inquiries you initiate with us (such as a customer service request or job application); (2) communicate information that we believe to be of interest to you via email; (3) improve our products and services; (4) fulfill your requests to share information you find on the Website with friends/other parties you have designated; (5) identify relevant advertisements to display.

We do not sell your personal information to third parties.

We may use your information to notify you of important changes to the Website, new services, and special offers. If you do not want to receive such notices, you may opt out as instructed in the WonderHowTo Terms of Use. Opting out may prevent you from receiving email messages regarding sales, updates, improvements, or special offers; provided, however that you may not opt-out of receiving notices required by applicable law via email and you hereby agree that our electronic signature on such notices is adequate. If we have provided any third party with your personal information at your election or request, you will have to contact the third-party directly with any opt-out request. If we provide any of the information collected from you with a third party at your election or request, their use of that information will be governed by their privacy policy. For example we use Google Analytics to help us understand how our visitors use the site. You can read more about how Google uses your personal information [here](https://www.google.com/intl/en/policies/privacy/). You can also opt-out of Google Analytics [here](https://tools.google.com/dlpage/gaoptout).

As the Service provides social functions, we may allow other users to access certain information you provide, such as profile information, your User Submissions, videos you have viewed, and subjects you are interested in. In addition, we allow RSS syndication of all public Service content.

We may release information, in our sole discretion, in response to the law, a court order, law enforcement request, or investigation or to protect our rights, property, or other interests, including those of our customers or other third parties or to prevent illegal activities or violations of the WonderHowTo Terms of Use.

In the event that we, in whole or in part, establish a partnership with another company, or are acquired by or merged with another company, collected information may be transferred to the partner or the acquiring or merging company.

Changing and Deleting

You can access your personal information through your profile and profile settings on the Website and delete, change or correct information; however, WonderHowTo cannot guarantee that all copies of such information will be immediately deleted from its servers. If you would like to delete your User Submissions in addition to your account, please contact us using the email address provided for privacy questions at the bottom of this Privacy Policy.

Child Protection

We do not offer the Website to, or target, persons under the age of 13. In compliance with the Children's Online Privacy Protection Act, any information we receive from people we believe to be under 13 will be purged from our database.

Security

We use industry standard security measures to protect against collected information. However, the Internet is not 100% secure and we accept no liability for any unintentional disclosure.

Links to Advertisers and Other Websites

Advertisements and links to third-party advertisers may be displayed on the Website or emailed to you. Third-party ad servers use technology to send, directly to your browser, the advertisements and links that appear on the Website. They automatically receive your IP address when this happens. They may also use other technologies (such as cookies, JavaScript, or web beacons) to measure the effectiveness of their advertisements and to personalize the advertising content. WonderHowTo does not provide any personally identifiable information to these third-party ad servers or ad networks without your consent. However, please note that if an advertiser asks WonderHowTo to show an advertisement to a certain audience and you respond to that advertisement, the advertiser or ad-server may conclude that you fit the description of the audience they are trying to reach. In addition, third-party advertisers may use information (not including your name, address, email address, or telephone number) about your visits to this and other websites in order to provide advertisements about goods and services of interest to you. If you would like more information about this practice and to know your choices about not having this information used by these companies, click [here](https://www.google.com/privacy_ads.html) and [here](https://www.networkadvertising.org/managing/opt_out.asp). If you are interested in more information about tailored browser advertising and how you can generally control cookies from being put on your computer to deliver tailored advertising, you may visit the [Network Advertising Initiative’s Consumer Opt-Out link](http://www.networkadvertising.org/choices), the [Digital Advertising Alliance’s Consumer Opt-Out link](http://www.aboutads.info/choices/), the [opt-out page of the European Interactive Digital Advertising Alliance](http://www.youronlinechoices.com/), or [TrustArc's Preference Manager](http://preferences-mgr.truste.com/) to opt-out of receiving tailored advertising from companies that participate in those programs. You may also use the links available in advertisements that appear on the Website. The information advertisers or other third parties collect is governed by their privacy policies, not by this Privacy Policy. In addition, User Submissions may contain links to other websites. We are not responsible for the privacy practices or the content of web publishers, advertisers, or other websites that may be linked to the Website.

In connection with the foregoing, we work with DigiTrust to set a first-party cookie in your browser to enable us and [DigiTrust Partners](http://www.digitru.st/participating-companies/)to collect web viewing data that includes visits to the Website and non-affiliated websites over time. This data may be used to infer whether you share interests with other users, and deliver advertising relevant to those inferences. Also, third parties whose products or services are accessible or advertised via the Website may place cookies or other tracking technologies on your computer, mobile phone, or other device to collect information about your use of the Website in order to (i) inform, optimize, and serve ads based on past visits to our websites and other sites and (ii) report how our ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to our websites and use of our Services. We also allow other third parties (e.g., ad networks and ad servers such as Google Analytics, DoubleClick and others) to serve tailored ads to you on the Services, other sites, and in other applications, and to access their own cookies or other tracking technologies on your computer, mobile phone, or other device you use to access the Services. We neither have access to, nor does this Policy govern, the use of cookies or other tracking technologies that may be placed on your computer, mobile phone, or other device you use to access the Website by non-affiliated, third-party ad technology, ad servers, ad networks or any other non-affiliated third parties. Those parties that use these technologies, including DigiTrust, may offer you a way to opt out of ad targeting as described above. You may receive tailored advertising on your computer through a web browser.

Do Not Track

We do not recognize or respond to browser-initiated "Do Not Track" (DNT) signals, as the Internet industry is currently still working toward defining exactly what DNT means, what it means to comply with DNT, and a common approach to responding to DNT. To learn more about Do Not Track, you can do so [here](http://allaboutdnt.com/).

Acceptance of Privacy Policy

By using the Website, you are accepting the then-current Privacy Policy, which may be updated from time to time. Any changes to the Privacy Policy will be posted here and are effective upon posting.

Fruit Ninja

**Privacy Policy**

**Effective Date: January 24, 2019**

At FruitNinja.io (“Fruit Ninja”, “we,” “us,” or “our”), we understand the importance of maintaining your privacy, and we, therefore, strive to provide our service with your protection in mind. This Privacy Policy applies to your use of our service whether accessed via computer or mobile device (the “Service”) on our owned and operated websites, mobile applications, and other properties on which a link to this Privacy Policy is provided (collectively, “Fruit Ninja”). This Policy does not apply to third-party properties that contain other privacy policies.

If you have any questions regarding this Privacy Policy, please at support at Fruit Ninja@gmail.com

**YOUR ACCEPTANCE**

In accessing the Service and/or the Fruit Ninja Web Pages, you accept all the terms and conditions of this Privacy Policy. Accordingly, we ask that you bookmark and periodically review this Privacy Policy to ensure continuing familiarity with the most current version. If you do not agree with the terms and conditions of this Privacy Policy, we request that you immediately cease using and accessing the Service and/or the Fruit Ninja Web Pages.

**INFORMATION WE COLLECT**

Fruit Ninja collects information from you in two ways: information you give to us, and information that we gather from your use of our Service, collectively known as “Personally Identifiable Information” or “PII”. PII, as described in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Such information is made up of “Personal Information” and “Non-Personal Information.”

“Personal Information” means information that you provide to us that personally identifies you, such as your first and last name, email address, physical address, telephone number, billing information, or social security number.

“Non-Personal Information” means information that does not specifically identify you.

**The information you give to us.**

We collect information that you give to us. For example, as part of our Service, you may elect to provide us with your email address or other information to receive newsletters and other notifications about certain features of our Service. Such registration may include your disclosure to us of Personal Information.

**Information we gather from your use of our Service.**

We, like many websites and applications, collect information about what parts of our Service you use and how you use them. Information we may gather includes, but is not limited to:

* Computer or browser information such as your system activity, the domain name of the web site from which you linked to our Service and/or the Fruit Ninja Web Pages, the time and duration of your use of our Service and any queries, browser type, and browser language.
* Device information such as your hardware model, operating system, operating system version, mobile device type, unique identifiers from your computer or mobile device, application download information, and/or IP address.
* Location information such as your geolocation when you use our Service from a mobile device and/or mobile application. We may ask for you to manually provide precise location information or to enable your mobile device to send us precise location information.

We may use unique identifiers, Flash cookies, web beacons, web server log information, or other technologies to collect information about you. In addition to the information that we collect from you for our own Service, we may collect information from you for third parties for purposes such as ad targeting, optimization, and reporting.

**OUR INFORMATION USE**

We collect information from you and our other users to administer our business activities and to measure and improve our Service. In addition, information collected from end-users may be used in aggregate form to, among other things, determine the total number of end-users who are using our Service, diagnose and fix compatibility problems or other problems with our Service, and perform statistical analyses to enable us to build higher quality, more useful online services and content. We may use the information collected from you to show advertising and promotions tailored to your interests. If you submit a request for information about Fruit Ninja through our web site, we may use your e-mail address to assist you with any issues you may have or to send you an e-mail that gives you the opportunity to elect to receive periodic e-mail alerts from Fruit Ninja regarding developments at the company. In addition, if you elect to receive promotional information from Fruit Ninja by registering for our newsletter and other notifications, we will use the information you provided to Fruit Ninja to send you only promotions that will be most relevant to you.

We may also use your e-mail address to send you important notices. Because this information is important to your use of our Service, you may not opt out of receiving these communications.

We may combine your Personal Information that we have with other information that we obtain from business partners or other companies. We may also combine your Personal Information with Non-Personal Information. If we do so, the combined information will be treated as Personal Information for as long as it remains combined.

**INFORMATION SHARING AND DISCLOSURE**

In providing our Service to you, we may find it necessary or beneficial to share your information with our partners, including our advertising, services and content partners (collectively, “Partners”) or allow such Partners to gather information directly from you.

Some of this information that you provide to us or our Partners may include your Personal Information. We may share your Personal Information with third parties in certain circumstances including the following situations:

* Consent: We will share Personal Information with third-parties when we have your consent to do so.
* Partners: We provide your Personal Information to Partners who work with us to provide our Service or provide services outside of and/or unrelated to the Fruit Ninja Web Pages or Service. Our Services with which our Partners may assist us to include among other things, communicating with you about new or existing Fruit Ninja or third-party services, creating or maintaining our databases, researching or analyzing our users, or processing payment card information.
* Affiliates: We may share your Personal Information with any and all of our Affiliates. “Affiliates” means any entity controlled by, controlling, or under common control with FruitNinja.io. Our Affiliates will use and distribute your information in accordance with the terms of this Privacy Policy.
* Legal Issues:  Fruit Ninja will use your Personal Information to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. We will also use or share your Personal Information in order to prevent, or take action regarding any illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Service, or as otherwise required by law even without a subpoena, warrant, or court order.
* Acquisition or Merger: If in the future we sell or transfer our assets or portions of our business, or if we experience a change in control, reorganization or liquidation, we may transfer information to our successor or buyer, subject to the terms of this Privacy Policy.

We reserve the right to share your Non-Personal Information publicly and with others. Examples of public information disclosures include providing anonymous reports to our Partners, such as the number of users who searched for “used cars” or how many users clicked on a particular listing or advertising on our Fruit Ninja Web Pages. In addition, some of the Non-Personal Information is provided to our Partners for uses such as calculating amounts owed by or to such Partners, or helping such Partners improve their services, amongst others.

Transfers of your information shall at all times be in accordance with applicable law. Fruit Ninja disclaims any liability or obligation as a result of any third-party actions or omissions concerning your information. We urge you to contact third parties directly with any issues you may have concerning their use of your information.

**COOKIES AND WEB BEACONS**

When you visit an Fruit Ninja Web Page and/or Service, a cookie that uniquely identifies your browser may be sent to your computer or mobile device. A “cookie” is a small file containing your preferences that are sent to your browser and sent back by your browser each time your browser accesses our servers. Cookies that we may use may only be read by the server that placed them there. We use cookies to improve the quality of our Service (for example, by fulfilling your language, filtering and other preferences) and to better understand how people interact with our Service (for example, by tracking user trends and patterns of how people search). Most browsers are initially set up to accept cookies. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some aspects of the Service may not function properly without cookies. If you would like more information about cookies and how to control and delete cookies in various browsers, such as Internet Explorer, Firefox, Safari, Opera and Chrome, please [click here](http://www.aboutads.info/consumers/).

We currently use the services of web analytics companies to help us measure the effectiveness of our Service, including the advertising on the Service. To do this, we allow the web analytics companies to include Web beacons and cookies on the Fruit Ninja Web Pages. The type of information collected via such Web beacons and cookies includes search terms, search parameters, click-throughs by users, and other similar information. By supplementing our records, this information helps us learn things like user preferences, popular search categories, click-through rates, how to improve our Service, and what kinds of offers our users like to see. Although our web analytics companies log this information on our behalf, we control how that data may be used.

Most, if not all, of the advertisements appearing on the Service, are delivered to you by one of our Web advertising partners (“Ad Serving Partners”). In the course of delivering such advertisements, our Ad Serving Partners may place or recognize a unique cookie on your browser, or place web beacons, JavaScript or other similar technologies on our Service for the purpose of collecting information. Thereafter, information about your visits to the Service, such as your search terms or phrases or the number of times you have viewed an advertisement (but not your name, address, or other Personal Information), is used to deliver targeted advertisements to you, a practice commonly known as “behavioral advertising.” The information collected by our Ad Serving Partners through cookies, web beacons or other similar technologies is anonymous, and our Ad Serving Partners are not authorized to collect any Personal Information about you. For more information about cookies please [click here](http://www.aboutads.info/consumers/). To “opt-out” of receiving cookies from certain of our Ad Serving Partners, please [click here](http://optout.networkadvertising.org/?c=1).

**Google**

Google’s advertising requirements can be summed up by Google’s Advertising Principles. They are put in place to provide a positive experience for users – <https://support.google.com/adwordspolicy/answer/1316548?hl=en>

Google, as a third-party vendor, uses cookies to serve ads on our site. Google’s use of the DART cookie enables it to serve ads to our users based on previous visits to our site and other sites on the Internet. Users may opt-out of the use of the DART cookie by visiting the Google Ad and Content Network privacy policy.

**CONFIDENTIALITY AND SECURITY**

We recognize our responsibility to protect the Personal Information you entrust to us. Here is how we protect your information:

* We do not use vulnerability scanning and/or scanning to PCI standards.
* We only provide articles and information. We never ask for credit card numbers.
* We do not use Malware Scanning.

Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems and are required to keep the information confidential. In addition, all sensitive information, including credit card if you do provide that to us, is encrypted via Secure Socket Layer (SSL) technology.

We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information. We maintain physical, electronic and procedural safeguards that comply with applicable law to guard your information. While we take precautions against possible breaches in our Service and customer databases, no website or Internet transmission is completely secure.

Accordingly, we cannot guarantee that unauthorized access, hacking, data loss, or other breaches will never occur. Your use of our Service and the Fruit Ninja Web Pages is at your own risk. We urge you to take steps to protect your Personal Information when you are on the Internet by changing your passwords often using a combination of letters and numbers, and make sure you use a secure Internet browser.

**THIRD-PARTY PRACTICES**

When users submit a search query on our Service, Non-Personal Information, such as IP addresses and search terms or phrases, is transmitted to certain Partners with whom Fruit Ninja has subcontracted so that those Partners can deliver responsive Internet search results, advertising, or other services and, in some cases, for the internal data reporting purposes of those Partners. Our Partners are obligated by applicable law to protect the privacy of certain types of data; however, we are not responsible for their actions or omissions, including the manner in which they use information that they receive from us. Nevertheless, if you feel that any of our Partners, or any third party who claims association with Fruit Ninja, is improperly collecting or using information about you, we urge you to contact them directly and also to inform us by e-mailing us at Fruit Ninja@gmail.com

**REGARDING CHILDREN**

**COPPA**

We comply with the Children’s Online Privacy Protection Act (COPPA). For more information about COPPA and children’s privacy, please click here. When we use the term “parent” below, we mean to include legal guardians.

***Children under the age of 13***

Our Service is not directed to children under the age of 13. If you are under the age of 13, you may not give us any Personal Information and you may not sign up for or participate in any aspect of our Service. Except as may be required by law, we will not knowingly collect, maintain, or disclose any Personal Information from children under the age of 13.

We do not intentionally gather Personal Information about visitors or end-users who are under the age of 13. If you believe that we have collected Personal Information about a visitor or end-user who is under the age of 13, please contact us at Fruit Ninja@gmail.com, and such Personal Information will be deleted.

***Children between the ages of 13 and 18***

If you are between the ages of 13 and 18, please be sure to read this Privacy Policy with your parent and get his or her permission before you give us any of your Personal Information.

***Information for Parents***

We encourage parents to spend time online with their children to become familiar with the types of content available on the internet, including the Fruit Ninja Web Pages. Parents should regularly oversee their children’s use of e-mail and other online communications and transactional features. Control tools are available from online services and software manufacturers that can help provide a safe online environment for kids.

We do not require a child to disclose more information than is reasonably necessary to participate in the Service as a condition of participation. Parents may request a review and/or removal of their child’s Personal Information at any time by contacting us at Fruit Ninja@gmail.com and providing us with the same screen name, password, and e-mail address that their child submitted. To protect the child’s privacy and security, we will take reasonable steps to verify the parent’s identity before granting him or her access to the child’s Personal Information.

**California Online Privacy Protection Act**

CalOPPA is the first state law in the nation to require commercial websites and online services to post a privacy policy. The law’s reach stretches well beyond California to require any person or company in the United States (and conceivably the world) that operates websites collecting Personally Identifiable Information from California consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals or companies with whom it is being shared. – See more at [http://consumercal.org/california-online-privacy-protection-act-caloppa/](https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/)

According to CalOPPA, we agree to the following:

* Users can visit our site anonymously.
* Once this privacy policy is created, we will add a link to it on our home page or as a minimum, on the first significant page after entering our website.
* Our Privacy Policy link includes the word ‘Privacy’ and can easily be found on the page specified above.
* You will be notified of any Privacy Policy changes: On our Privacy Policy Page
* Can change your personal information: By emailing us or by logging into your account should we provide that feature.
* We honor Do Not Track signals and Do Not Track, plant cookies, or use advertising when a Do Not Track (DNT) browser mechanism is in place.

**Fair Information Practices**

The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

To be in line with Fair Information Practices we will notify you via email within 7 business days should a data breach occur. We also agree to the Individual Redress Principle which requires that individuals have the right to legally pursue enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or government agencies to investigate and/or prosecute non-compliance by data processors.

**CAN-SPAM Act**

The CAN-SPAM Act is a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have emails stopped from being sent to them, and spells out tough penalties for violations.

We collect your email address in order to:

* Send information, respond to inquiries, and/or other requests or questions

To be in accordance with CAN-SPAM, we agree to the following:

* Not use false or misleading subjects or email addresses.
* Identify the message as an advertisement in some reasonable way.
* Include the physical address of our business or site headquarters.
* Monitor third-party email marketing services for compliance, if one is used.
* Honor opt-out/unsubscribe requests quickly.
* Allow users to unsubscribe by using the link at the bottom of each email.

If at any time you would like to unsubscribe from receiving future emails, you can email us at reporting Fruit Ninja@gmail.com or follow the instructions at the bottom of each email and we will promptly remove you from ALL correspondence.

**INFORMATION FOR VISITORS FROM THE EUROPEAN UNION (EU)**

This section of the Privacy Policy applies only if you use our website or Services covered by the Privacy Policy from a country that is a Member State of the European Union, and it supplements the information in the Privacy Policy.

Diversify Media, Inc. is the data controller for processing of information defined as personal data under applicable data protection law (“Personal Data”).

**LEGAL BASIS FOR DATA PROCESSING**

We process Personal Data for the purposes set out in the Privacy Policy. Our legal basis to process Personal Data includes processing that is: necessary for the performance of the contract between you and Diversify Media, Inc. (for example, to provide you with the Services you request and to identify and authenticate you so you may use the website); necessary to comply with legal requirements (for example, to comply with applicable accounting rules and to make mandatory disclosures to law enforcement); necessary for our legitimate interests (for example, to manage our relationship with you and to improve the website and our Services); and based on consent by our customers (for example, to communicate with you about our products and services and provide you with marketing information), which may subsequently be withdrawn at any time by contacting us (using the contact instructions below) without affecting the lawfulness of processing based on consent before its withdrawal.

**EU DATA SUBJECT RIGHTS**

The EU General Data Protection Regulation (GDPR) provides certain rights for EU data subjects. You may decline to share certain personal information with us, in which case we may not be able to provide some of the features and functionality of our Services. These rights include, in accordance with applicable law, the right to object to or request the restriction of processing of your Personal Data, and to request access to, rectification, erasure, and portability of your own Personal Data. Requests should be submitted by contacting us (using the contact instructions below).

We will make commercially reasonable efforts to provide you reasonable access to your personal information within 30 days of your access request to the contact address below. We provide this access so that you may review, make corrections, or request deletion of your personal information. If we cannot honor your request within 30 days, we will inform you when we will be able to provide such access. If for some reason access is denied, we will provide an explanation as to why access is denied. When technically feasible, at your request, we will provide your personal data to you or transmit it directly to another controller.

We will retain your personal information for as long as it is reasonably necessary for the purposes set out in the Privacy Policy, considering the time period reasonably necessary to: provide the Services to you; exercise the choices and rights you have requested; comply with our contractual obligations; enforce our terms for use of the Services; and, comply with legal and regulatory requirements.

If you have any unresolved privacy concern that we have not addressed satisfactorily after contacting us, you have the right to contact the appropriate EU Data Protection Authority and lodge a complaint.

**THIRD PARTY ONLINE ADVERTISING**

We enable certain third-party advertising exchanges to place advertisements on our sites. With your consent, those advertising exchanges collect your IP address and/or a unique advertising ID that is used by the advertising exchange to identify you across the internet.

The European Digital Advertising Alliance {“EDAA”} has developed a guide to online behavioral advertising and has developed an opt-out page to manage online behavioral advertising preferences with EDAA member companies available at [www.YourOnlineChoices.com](http://www.youronlinechoices.com/). To find out more about how you can manage cookies and the other similar technologies, see [Managing Cookies](http://www.allaboutcookies.org/manage-cookies/).

**ADDITIONAL TERMS**

**Changes to this Privacy Policy**

We may revise this Privacy Policy from time to time. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice. Your continued use of our Service after such change has been made will signify your acceptance of such change.

**California Privacy Rights Under California Civil Code Section 1798.83**

California Civil Code Section 1798.83 permits end users who are California residents to request certain information regarding our disclosure of Personal Information to third parties for their direct marketing purposes. To make such a request, please send us an e-mail at Fruit Ninja@gmail.com.

**Contact Us**

If you have any questions about this Privacy Policy, please feel free to contact us by e-mail at Fruit Ninja@gmail.com.

Winscp

**What information do we collect?**

We can collect information from you when you visit our site, install or use WinSCP application. People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used.

**Visiting winscp.net**

When registering on our site, as appropriate, you may be asked to enter your: name, e-mail address or location. You may, however, visit our site anonymously.

After donating to WinSCP, as appropriate, you may be asked to enter your: name, e-mail address, mailing address or donation entry details.

Third party vendors, including Google, use cookies to serve ads on our site. Google’s use of the DART cookie enables it to serve ads to our users based on their visit to our site and other sites on the Internet. Users may opt-out of the use of the DART cookies by visiting the Google ad and content network Privacy policy. Users may opt out of DoubleClick’s use of cookies by visiting the DoubleClick opt-out page.

**Installing WinSCP application**

When installing WinSCP, we might collect anonymous information about the number of initiated and finished installations per geo-location and language. No private information is collected. WinSCP installer might offer you to install a third party application along with WinSCP, in such a case we collect also statistics for its installations. Note that before deciding to install any third party application, you are required to agree to its separate and independent Terms of use and Privacy policy.

**Using WinSCP application**

When using WinSCP application, we might collect anonymous [WinSCP usage statistics](https://winscp.net/eng/docs/usagestatistics). You may, however, opt-out from providing WinSCP usage statistics or from WinSCP automatic check for application updates.

Advertisement

**What do we use your information for?**

Any of the information we collect from you may be used in one of the following ways:

* **To personalize your experience** (your information helps us to better respond to your individual needs)
* **To improve our website and our application**(we continually strive to improve our offerings based on the information and feedback we receive from you)
* **To process transactions** (your information, whether public or private, will not be sold, exchanged, transferred, or given to any other company for any reason whatsoever, without your consent, other than for the express purpose of delivering the purchased product or service requested.)
* **To administer a contest, promotion, survey or other site feature**

**How do we protect your information?**

We use PayPal to process your payments. PayPal offers the use of a secure server. All supplied sensitive information is transmitted via Transport Layer Security (TLS) or Secure Socket Layer (SSL) technology and then encrypted into our Payment gateway providers database only to be accessible by those authorized with special access rights to such systems, and are required to keep the information confidential. Please refer also to PayPal Privacy policy for details.

After a transaction, your private information (credit cards, social security numbers, etc.) will not be stored on our servers.

**Do we use cookies?**

Yes, on winscp.net we use cookies. Cookies are small files that a site or its service provider transfers to your computers hard drive through your Web browser (if you allow) that enable the sites or service providers systems to recognize your browser and capture and remember certain information.

We use cookies to compile aggregate data about site traffic and site interaction so that we can offer better site experiences and tools in the future.

Note that you can change your browser settings to disable cookies if you have privacy concerns.

**Do we disclose any information to outside parties?**

We do not sell, trade, or otherwise transfer to outside parties your personally identifiable information. This does not include trusted third parties who assist us in operating our website, conducting our business, or servicing you, so long as those parties agree to keep this information confidential. We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others rights, property, or safety. However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

**Third party links**

Occasionally, at our discretion, we may include or offer third party products or services on our website. These third party sites have separate and independent privacy policies. We therefore have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our site and welcome any feedback about these sites.

Advertisement

**California online privacy protection act compliance**

Because we value your privacy we have taken the necessary precautions to be in compliance with the California Online Privacy Protection Act. We therefore will not distribute your personal information to outside parties without your consent.

All registered users of our site may make any changes to their information at anytime by logging into the forum and going to the *Profile* page.

**Your consent**

By using our site or installing or using WinSCP, you consent to our Privacy policy.

**Warrant canary**

We have not placed any backdoors into our software and have not received any requests for doing so. Pay close attention to any modifications to the previous sentence.

Learn about [Warrant canary](https://en.wikipedia.org/wiki/Warrant_canary).

**Changes to our Privacy policy**

If we decide to change our Privacy policy, we will post those changes on this page, and update the Privacy policy modification date below.

This policy was last modified on **2015-11-15**.

— [WinSCP team](https://winscp.net/)

*This policy is based on*[*Free Privacy Policy Generator*](https://www.freeprivacypolicy.com/)

SOFTONIC PRIVACY POLICY

WHEN THIS POLICY APPLIES?

We have made this policy as short and easy to understand as possible, so please take your time to read it so you can have all the information to decide whether you want to sign up and share your data with Softonic.

This policy applies to www.softonic.com, its subdomains and other web sites and services where this Privacy Policy is referred or made accessible for you to read and accept.

The personal data to which we have access is the data that you will voluntarily provide upon sign up as required for the use of certain services.

You can easily sign up via the available social media sign up options or by filling out the necessary online forms where this option is available. Fields marked with an asterisk (\*) are mandatory. Lack to provide the mandatory data will preclude you from signing up.

Please refer to our [Cookies Policy](https://hello.softonic.com/cookies-policy/) to know how we and third parties process data obtained by means of cookies and similar technologies.

WHO AM I SHARING MY DATA WITH AND WHO IS THE DATA “CONTROLLER”?

A data controller is an entity that you provide data with and decides on the purpose of the data, provided your prior consent or another legal basis:

Corporate name: Softonic International, S.A.

Address: MediaTIC building, Calle Roc Boronat, 117, 6th floor, 08018 Barcelona, Spain

Phone number: +34 936 012 700

Email address: [privacy@softonic.com](mailto:privacy@softonic.com)

Data Protection Officer direct contact: [dpo@softonic.com](mailto:dpo@softonic.com)

Please do not hesitate to reach us by any of the means above for any question about data protection and privacy.

WHAT ARE THE PURPOSES OF DATA PROCESSING?

* If you subscribe, creation of a community of users interested in software, so you can share your opinion and preferred programs and solutions with other users. Note that third party privacy policies may apply (currently Softonic uses Discuss as public comment sharing platform. Please review its [Privacy Policy](https://help.disqus.com/en/articles/1717103-disqus-privacy-policy) for more information)
* To show you other users’ opinions about programs or solutions.
* If you subscribed to our newsletter, to inform you about reviews, news, tutorials, opinions, all related to the world of software.
* If you subscribed to our newsletter, to recommend you software, based on your interests, download history and navigation habits on the website.
* To study and analyze the information provided, as well as based on information obtained in an aggregate format for statistical and analytics purposes via cookies (see our [Cookies Policy](https://hello.softonic.com/cookies-policy/)for more info), in order to evaluate new trends, develop new services or check the result of an ad campaign.
* If you subscribed to our newsletter, to send you emails about updates, service announcements or as required to provide you with the subscribed service. This kind of communications do not have a commercial nature and we will inform you of how to unsubscribe on each communication.
* Provided your previous consent, to send you emails regarding the software sector.
* To address you properly on our emails (i.e dear “John Smith”).
* To create a user profile. We will not use your profile for automatic individual decision-making.
* To show you relevant ads on the website, newsletters and web notifications.
* To show you relevant ads in other websites and social networks that may be of your interest (see our [Cookies Policy](https://hello.softonic.com/cookies-policy/)at this regards).
* To check you are above 14 years old, so you can give us a valid consent to provide your data.
* To answer your questions, complaints and provide general support, if you contact us via our support portal, other online forms or directly via email.
* Provided you have voluntarily opted-in to receive our newsletter, you will receive customized ads on our newsletters.

We’ll keep your data as long as we don’t receive a deletion request from you and as long as permitted by Law. You can delete your Discuss account [here](https://privacyportal-cdn.onetrust.com/dsarwebform/bc2d3301-11a5-4de5-b15e-ce796187a352/9a049fa1-37af-4598-a87a-d0df2e2d904b.html), unsubscribe from our newsletter at any time via the link provided on the email. To unsubscribe from web push notification please follow [these steps](https://hello.softonic.com/faqs/) (section How to Disable Web Notifications).

WHAT’S THE LEGAL BASIS OF THE PROCESSING?

The legal basis for the processing of your data is your consent.

For children below 14 years old, we require the authorization of parents or guardians for signing up. Please contact us via email to [privacy@softonic.com](mailto:privacy@softonic.com)if you want your children to subscribe and we’ll provide you further instructions to do so.

WILL MY DATA BE SHARED WITH THIRD PARTIES?

**Third-party service providers.**Softonic has engaged with several trusted third parties-service providers (data processors) in order to provide the service. For instance, they provide us with services such as hosting, data management or direct marketing related services, so they need to access certain data on as needed strictly basis. Softonic requires all its providers to certify that they have adopted adequate organizational and security measures to comply with our data protection standards and require them to commit to adopting further legal safeguards. Where the relevant provider is located outside the Economic European Area (EEA), we require the adhesion to the US-EU Privacy Shield or the signature of EU standard clauses.

Below you’ll find a list of providers located outside the EEA, the country and the existence or absence of an adequacy decision by the EU Commission (when the EU Commission has determined that a certain country offers sufficient guarantees for the protection of personal data and privacy) and the relevant safeguards adopted.

*Google, Inc*. U.S. Adequacy decision in the framework of the EU-US Privacy Shield. Google is adherent to the Privacy Shield.

*Amazon.com Inc*. U.S. Adequacy decision in the framework of the EU-US Privacy Shield. Amazon is adherent to the Privacy Shield.

*Fastly, Inc.* U.S. U.S. Adequacy decision in the framework of the EU-US Privacy Shield. Oracle is adherent to the Privacy Shield.

Onesignal,*Inc*. U.S. Adequacy decision in the framework of the EU-US Privacy Shield. EU Standard Contractual Clauses (Processors)

*MailChimp, Inc* U.S. Adequacy decision in the framework of the EU-US Privacy Shield. EU Standard Contractual Clauses (Processors)

*Key Discovery Consulting, Inc*. Republic of the Philippines EU Standard Contractual Clauses (Processors)

Visit [https://www.privacyshield.gov](https://www.privacyshield.gov/)for more info about the Privacy Shield and to check that the above companies are adherent to.

**Legal reasons**: We may disclose personal information when we believe release is appropriate to comply with the law; enforce or apply our terms of use and other agreements; or protect our rights.

**Business Transfers**: As we continue to develop our business, we might sell or buy other companies, subsidiaries, or business units. In such transactions, user information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing privacy policies (unless, of course, you consent otherwise). Also, in the event that Softonic or substantially all of its assets are acquired, user information will, of course, be one of the transferred assets.

Please visit our [Cookies Policy](https://hello.softonic.com/cookies-policy/)to know the data we and third parties process via the usage of cookies and other similar technologies.

WHAT RIGHTS DO I HAVE?

You can have control over the data provided, including the ability to request your rights to access, rectify and delete, restrict the processing and to object certain processing (i.e unsubscribe from our newsletter). you may send us an email to [privacy@softonic.com](mailto:privacy@softonic.com)to request your rights. You can exercise your rights in you subscribed to Discuss [here](https://privacyportal-cdn.onetrust.com/dsarwebform/bc2d3301-11a5-4de5-b15e-ce796187a352/9a049fa1-37af-4598-a87a-d0df2e2d904b.html).

You can as well unsubscribe from receiving our newsletter at any time by clicking the relevant button at the bottom of any email we send you.

If you have subscribed to our web notification service you can opt-out at any time via your web browser following these [steps](https://get-support.softonic.com/customer/en/portal/articles/2873957-how-to-disable-web-notifications-chrome-firefox-and-safari-)

Please note that the exercise of your right to erasure or to object to certain data processing will not affect the lawfulness of processing based on your consent before withdrawal.

We will process your data to create a profile that will include the data you provide, along with data related to your behaviour in the web site, how you react to our email campaigns but will not be used for automatic individual decision-making purposes. This profile will be used to show you customized content and ads that will be more relevant to you. You can also opt-out from this type of processing at any time via your user area.

Visit the Spanish National Data Protection Authority [website](http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/ejercicio_derechos/index-iden-idphp.php)to learn more about your rights. Be informed that you have the right to lodge a complaint before the Spanish National Data Protection Authority especially if we have failed to comply with your request to exercise your rights.

IS MY DATA SECURED?

We have adopted adequate technical and organizational measures to avoid alteration, loss or unauthorized access to your data: We select only trusted and certified providers that process your data and we take care that they have taken strict measures too. We and our providers also use encryption protocols to access or transfer your data and techniques to anonymize data to mitigate the risks in case of a data leak.

HOW CAN I KNOW IF YOU CHANGE THIS POLICY?

We will inform you sufficiently in advance if there are important changes and require your consent if any of those changes impact your privacy rights.

Last Version 29 June 2020. © Softonic International, S.A.

Twint

Datenschutz und Transparenz haben für TWINT einen hohen Stellenwert. Wir möchten die Nutzerinnen und Nutzer an dieser Stelle in Kurzform darüber aufklären, welche Daten bei uns gespeichert und wozu sie verwendet werden. Rechtlich massgebend sind die[Allgemeinen Geschäftsbedingungen (AGB)](https://www.twint.ch/privatkunden/agb-app), die bei der Installation der App akzeptiert werden.

**Weitergabe von Daten**

TWINT gibt nie personenbezogene Daten an Dritte weiter. Personenbezogene Daten sind Daten, die einer einzelnen Person zugeordnet werden können. Einzige Ausnahme ist die Weitergabe von Daten an sogenannte Auftragsdatenbearbeiter, die im Auftrag von TWINT gewisse Daten bearbeiten.

**Sammlung und Auswertung von Daten**

Bei der Sammlung und Auswertung von Daten unterscheiden wir zwischen Nutzerinnen und Nutzern, die in der TWINT App ein Opt-in für Angebote von Dritten gemacht haben, und Nutzerinnen und Nutzern, die sich für ein Opt-out entschieden haben. Für Nutzerinnen und Nutzer mit Opt-out werden nur die Daten gesammelt, die für die Abwicklung der Zahlungen benötigt werden. Für Nutzerinnen und Nutzer mit Opt-in werden zusätzliche Daten gesammelt und ausgewertet. Diese Daten erlauben TWINT, den Nutzerinnen und Nutzern Angebote anzuzeigen, die möglichst gut zu ihnen passen.

Konkret wird erfasst und ausgewertet, bei welchem Händler eine Nutzerin oder ein Nutzer mit TWINT einkauft und welche Angebote sie oder er in der TWINT App anschaut, aktiviert und einlöst. Bei Nutzerinnen und Nutzern, die der TWINT App Zugriff auf die Standortfunktionalität ihres Smartphones geben, wird bei der aktiven Nutzung der TWINT App auch der Standort übermittelt. Dies dient dazu, den Nutzenden Angebote an Orten anzeigen zu können, an denen sie sich häufig aufhalten. Der Standort wird nicht übermittelt, wenn die TWINT App sich im Hintergrund befindet. Es findet kein so genanntes Background Tracking statt. Der Zugriff der TWINT App auf den Standort kann in den Einstellungen des Betriebssystems des Smartphones ein- und ausgeschaltet werden.

**Verwendung von Google Analytics**

Um die TWINT Apps laufend zu verbessern, wird in allen TWINT Apps – mit Ausnahme von UBS TWINT und ZKB TWINT – Google Analytics eingesetzt (die UBS und ZKB setzen keine bzw. eigene Tracking Tools ein). Mit Google Analytics wird gemessen, welche Inhalte die Nutzerin oder der Nutzer in der App öffnet. Dies hilft, Fehler zu erkennen und die Navigation in der TWINT App zu verbessern. Personenbezogene Daten werden nicht an Google übermittelt. Die IP-Adresse des Smartphones wird anonymisiert. Weiter haben die  Nutzerinnen und Nutzer die Möglichkeit, in den Einstellungen der TWINT App das Tracking auszuschalten (im Menü unter «Mehr» > «Allgemeine Geschäftsbedingungen»).

**Löschung der Daten**

Alle von TWINT gesammelten Daten werden spätestens nach vier Jahren gelöscht respektive anonymisiert. Standortdaten speichern wir nur ungenau ab (Radius 2–5 km) und löschen sie spätestens nach sechs Monaten. Von der Löschung bzw. Anonymisierung ausgenommen sind Daten, die von Gesetzes wegen länger aufbewahrt werden müssen, wie z. B. die Zahlungsdaten. Wenn eine Nutzerin oder ein Nutzer die TWINT App während zwei Jahren nicht mehr gebraucht hat, gehen wir davon aus, dass sie oder er die TWINT App gelöscht hat und löschen alle ihre bzw. seine Daten, die nicht von Gesetzes wegen länger aufbewahrt werden müssen. Das heisst: Alle zuvor aktivierten Coupons und Stempelkarten werden gelöscht.

DuckDuckGo

[**DuckDuckGo**](https://duckduckgo.com/?q=&t=i)**does not collect or share personal information.** That is our privacy policy in a nutshell. The rest of this page tries to explain why you should care

WHY YOU SHOULD CARE

SEARCH LEAKAGE  [[TOP](https://duckduckgo.com/privacy#top)]

At other search engines, when you do a search and then click on a link, your search terms are sent to that site you clicked on (in the [HTTP referrer header](https://duckduckgo.com/HTTP_referrer)). We call this sharing of personal information "search leakage."

For example, when you search for something private, you are sharing that private search not only with your search engine, but also with all the sites that you clicked on (for that search).

In addition, when you visit *any* site, your computer automatically sends information about it to that site (including your [User agent](https://duckduckgo.com/User_agent) and [IP address](https://duckduckgo.com/IP_Address)). This information can often be used to identify you directly.

So when you do that private search, not only can those other sites know your search terms, but they can also know that *you* searched it. It is this combination of available information about you that raises privacy concerns.

DuckDuckGo prevents search leakage by default. Instead, when you click on a link on our site, we route (redirect) that request in such a way so that it does not send your search terms to other sites. The other sites will still know that you visited them, but they will not know what search you entered beforehand.

At some other search engines (including us), you can also use an [encrypted version](https://duckduckgo.com/) ([HTTPS](https://duckduckgo.com/HTTP_Secure)), which as a byproduct doesn't usually send your search terms to sites. However, it is slower to connect to these versions and if you click on a site that also uses HTTPS then your search is sent. Nevertheless, the encrypted version does protect your search from being leaked onto the computers it travels on between you and us.

At DuckDuckGo, our encrypted version goes even further and automatically changes links from a number of major Web sites to point to the encrypted versions of those sites. It is modeled after (and uses code from) the [HTTPS Everywhere](https://www.eff.org/https-everywhere/) FireFox add-on. These sites include Wikipedia, Facebook, Twitter, and Amazon to name a few.

Another way to prevent search leakage is by using something called a [POST request](https://duckduckgo.com/?q=POST+request), which has the effect of not showing your search in your browser, and, as a consequence, does not send it to other sites. You can turn on POST requests on our [settings page](https://duckduckgo.com/settings), but it has its own issues. POST requests usually break browser back buttons, and they make it impossible for you to easily share your search by copying and pasting it out of your Web browser's address bar.

Finally, if you want to prevent sites from knowing you visited them at all, you can use a proxy like [Tor](https://www.torproject.org/). DuckDuckGo actually operates a [Tor exit enclave](https://help.duckduckgo.com/privacy/tor-exit-enclave/), which means you can get end to end anonymous and encrypted searching using Tor & DDG together.

You can enter !proxy domain into DuckDuckGo as well, and we will route you through a proxy, e.g. [!proxy breadpig.com](https://duckduckgo.com/?q=!proxy+breadpig.com). This feature is part of our [!bang syntax](https://duckduckgo.com/bang). Unfortunately, proxies can also be slow, and free proxies (like the one we use) are funded by arguably excessive advertising.

Because of these drawbacks in HTTPS, POST and proxies we decided to take the redirect approach to combat search leakage. However, we leave the choice up to you. You can deviate from the default on our [settings page](https://duckduckgo.com/settings) by toggling the redirect or address bar settings. You can also use our [encrypted version](https://duckduckgo.com/).

SEARCH HISTORY  [[TOP](https://duckduckgo.com/privacy#top)]

Other search engines save your search history. Usually your searches are saved along with the date and time of the search, some information about your computer (e.g. your [IP address](https://duckduckgo.com/IP_Address), [User agent](https://duckduckgo.com/User_agent) and often a unique identifier stored in a [browser cookie](https://duckduckgo.com/HTTP_cookie)), and if you are logged in, your account information (e.g. name and email address).

With only the timestamp and computer information, your searches can often be traced directly to you. With the additional account information, they *are* associated directly with you.

Also, note that with this information your searches can be tied together. This means someone can see everything you've been searching, not just one isolated search. You can usually find out a lot about a person from their search history.

It's sort of creepy that people at search engines can see all this info about you, but that is not the main concern. The main concern is when they either a) release it to the public or b) give it to law enforcement.

Why would they release it to the public? AOL famously released supposedly anonymous search terms for research purposes, except they didn't do a good job of making them completely anonymous, and they were ultimately [sued over it](https://yro.slashdot.org/story/06/09/25/2150209/AOL-Subscribers-Sue-Over-Release-Of-Search-Data). In fact, almost every attempt to anonymize data has similarly been later found out to be much less anonymous than initially thought.

The other way to release it to the public is by accident. Search engines could lose data, or get hacked, or accidentally expose data due to security holes or incompetence, all of which has happened with personal information on the Internet.

Why would search engines give your search history to law enforcement? Simply because law enforcement asked for it, usually as part of a legal investigation. If you read privacy policies and terms of service carefully you will notice that they say they can give your information on court order.

This makes sense because they may be legally obligated to do so. However, search engines are not legally obligated to collect personal information in the first place. They do it on their own volition.

The bottom line is if search engines have your information, it could get out, even if they have the best intentions. And this information (your search history) can be pretty personal.

For these reasons, DuckDuckGo takes the approach to not collect any personal information. The decisions of whether and how to comply with law enforcement requests, whether and how to anonymize data, and how to best protect your information from hackers are out of our hands. Your search history is safe with us because it cannot be tied to you in any way.

INFORMATION

INFORMATION NOT COLLECTED  [[TOP](https://duckduckgo.com/privacy#top)]

When you search at DuckDuckGo, we don't know who you are and there is no way to tie your searches together.

When you access DuckDuckGo (or any Web site), your Web browser automatically sends information about your computer, e.g. your [User agent](https://duckduckgo.com/User_agent) and [IP address](https://duckduckgo.com/IP_Address).

Because this information could be used to link you to your searches, we do not log (store) it at all. This is a very unusual practice, but we feel it is an important step to protect your privacy.

It is unusual for a few reasons. First, most server software auto-stores this information, so you have to go out of your way not to store it. Second, most businesses want to keep as much information as possible because they don't know when it will be useful. Third, many search engines actively use this information, for example to show you more targeted advertising.

Another way that your searches are often tied together at other search engines are through [browser cookies](https://duckduckgo.com/HTTP_cookie), which are pieces of information that sit on your computer and get sent to the search engine on each request. What search engines often do is store a unique identifier in your browser and then associate that identifier with your searches. At DuckDuckGo, no cookies are used by default.

In response to efforts by the [EFF](https://duckduckgo.com/Electronic_Frontier_Foundation) and others, the major search engines have begun "anonymizing" their search log data after periods of time. Sure, this is better than not doing so, but you should note that this does not make your search history anonymous in the same way that it is at DuckDuckGo.

What search engines generally do when they anonymize data is get rid of part of your IP address or turn it into something that doesn't look exactly like an IP address. And they do the same thing for uniquely identifying cookies.

However, in many cases, this so-called anonymous data can still tie your searches together, which can be used to reconstruct who you are and what you searched for. Additionally, search engines usually are silent on what they do with the User agent, which [has been shown](https://www.eff.org/deeplinks/2010/01/tracking-by-user-agent) to also have enough information to often be personally identifiable, especially if isolated to a particular search session (day).

INFORMATION COLLECTED  [[TOP](https://duckduckgo.com/privacy#top)]

At DuckDuckGo, no cookies are used by default. If you have changed any [settings](https://duckduckgo.com/settings), then cookies are used to store those changes. However, in that case, they are not stored in a personally identifiable way. For example, the large size setting is stored as 's=l'; no unique identifier is in there. Furthermore, if you prefer not to use cookies to store settings, you can use [URL parameters](https://duckduckgo.com/params) instead.

Additionally, if you use our [!bang syntax/dropdown](https://duckduckgo.com/bang), which bangs you use are stored in a cookie so that we can list your most frequently used ones on top of the !bang dropdown box. Just like the other settings, this information is not saved on our servers at all, but resides solely on your computer. There is also a [setting](https://duckduckgo.com/settings) to turn this off, which you can also set via a [URL parameter](https://duckduckgo.com/params). Particular searches are of course not stored. An example cookie might look like: php=2&yelp=19&java=4.

We also save searches, but again, not in a personally identifiable way, as we do not store IP addresses or unique User agent strings. We use aggregate, non-personal search data to improve things like misspellings.

Similarly, we may add an affiliate code to some eCommerce sites (e.g. Amazon & eBay) that results in small commissions being paid back to DuckDuckGo when you make purchases at those sites. We do not use any third parties to do the code insertion, and we do not work with any sites that share personally identifiable information (e.g. name, address, etc.) via their affiliate programs. This means that no information is shared from DuckDuckGo to the sites, and the only information that is collected from this process is product information, which is not tied to any particular user and which we do not save or store on our end. It is completely analogous to the search result case from the previous paragraph--we can see anonymous product info such that we cannot tie them to any particular person (or even tie multiple purchases together). This whole affiliate process is an attempt to keep advertising to a minimal level on DuckDuckGo.

Finally, if you [give us feedback](https://duckduckgo.com/feedback), it may be stored in our email. However, you can give anonymous feedback (by not entering your email or other personal info on the feedback form).

INFORMATION SHARED  [[TOP](https://duckduckgo.com/privacy#top)]

If you turn redirects off in the [settings](https://duckduckgo.com/settings) and you don't either turn POST on or use our [encrypted site](https://duckduckgo.com/), then your search could leak to sites you click on. Yet as explained above, this does not happen by default.

Also, like anyone else, we will comply with court ordered legal requests. However, in our case, we don't expect any because there is nothing useful to give them since we don't collect any personal information.

OTHER

OTHER SEARCH ENGINES  [[TOP](https://duckduckgo.com/privacy#top)]

If you care about search privacy, you might also want to check out these other search engines that take it seriously by default.

* [Ixquick](https://ixquick.com/) [[privacy policy](https://ixquick.com/eng/protect-privacy.html)]

Each does things a bit differently in terms of privacy and very differently in terms of results. And not all go as far as DuckDuckGo in some aspects. However, none store your personal information by default, which make them all pretty safe in our opinion.

UPDATES  [[TOP](https://duckduckgo.com/privacy#top)]

If this policy is substantively updated, we will update the text of this page and provide notice to you at <https://duckduckgo.com/about> by writing '(Updated)' in red next to the link to this page (in the footer) for a period of at least 30 days.

FEEDBACK  [[TOP](https://duckduckgo.com/privacy#top)]

I ([Gabriel Weinberg](https://duckduckgo.com/?q=Gabriel+Weinberg)) am the founder of Duck Duck Go and personally wrote this privacy policy. If you have any questions or concerns, please [submit feedback](https://duckduckgo.com/feedback).

Add DuckDuckGo to Chrome

Tor Browser

PRIVACY POLICY

- ​What information we collect

- 1. Personal Information:

- We do NOT collect any Personal Information about you. “Personal Information” means personally identifiable information, such as your name, email address, physical address, calendar entries, contact entries, files, photos, etc.

- 2. Non-Personal Information:

- We collect non-personal information about your use of our Apps and aggregated information regarding the usages of the Apps. “Non-Personal Information” means information that is of an anonymous nature, such as the type of mobile device you use, your mobile devices unique device ID, the IP address of your mobile device, your mobile operating system, the list of system applications and currently installed applications, and information about the way you use the Applications.

- 3. Location Services:

- We do NOT request, collect, or access your location information.

THIRD PARTY APPS / LINKS

- Inside our apps or services we display ads / links to other companies or mobile applications. When you click on ads / links of third parties in our apps or services, you may leave the app or service. We do not responsible for the privacy practices adopted by third parties. We recommend that you read their privacy policies.

SECURITY

- We are very concerned about safeguarding the confidentiality of your information. We do not collect Personal Information, and we employ administrative, physical and electronic measures designed to protect your Non-Personal Information from unauthorized access and use.

Your Privacy

- We do not store or retain any personal information that can be used to identify you (the end user), unless specifically stated in the application (for example, an e-mail address used for account registration). No data specific to the end user will be shared or sold to third parties. We have no interest in housing and storing users personal information or data.

CONTACT

- If you have any questions or comments about this Privacy Policy, or any other issues regarding our apps or services, Mail at contact.approsoftllc@gmail.com

FAZ

Inhaltsverzeichnis

1. Wir sind verantwortlich für Ihre Daten

2. Wie sicher sind Ihre Daten?

3. Unser Datenschutzbeauftragter

4. Was sind personenbezogene Daten?

5. Was sind Pflichtangaben oder Pflichtfelder?

6. Wofür werden Ihre Daten verarbeitet?

7. Jederzeitiges Widerspruchs- und Widerrufsrecht

8. Cookies und andere Technologien

9. Soziale Medien

10. Datenbank zur Verhinderung missbräuchlicher Nutzung / Erlöszuordnung

11. Fremde Inhalte und Dienste von Dienstleistern

12.Wie können Sie Ihre Datenschutzrechte wahrnehmen?

13. Änderungen

1. Wir sind verantwortlich für Ihre Daten.

Als Besucher unserer Website und bei der Inanspruchnahme unserer Leistungen erwarten Sie nicht nur von unseren Nachrichten und unseren Verlagsprodukten, sondern auch bei der Verarbeitung Ihrer personenbezogenen Daten ein hohes Maß an Qualität und Kompetenz.

Wir sind verantwortlich für den Umgang mit Ihren Daten, die wir nach Ihren Wünschen und nach den Vorgaben der deutschen und EU-Datenschutzgesetze verarbeiten. Ihre personenbezogenen Daten werden von uns nur verarbeitet, sofern eine Rechtsvorschrift dies erlaubt.

*Wir*, das ist die Frankfurter Allgemeine Zeitung GmbH, Hellerhofstraße 2-4, 60327 Frankfurt am Main (im Folgenden: FAZ, wir). Sie erreichen uns neben der vorgenannten Postanschrift auch per E-Mail unter [info@faz.net](mailto:info@faz.net).

Wir binden bei unserer Tätigkeit auch Dienstleister ein. Bei der unten beschriebenen Verarbeitung Ihrer Daten können daher auch diese Dienstleister Ihre Daten empfangen und in unserem Auftrag für die unten angegebenen Zwecke verarbeiten. Zu unseren Dienstleistern gehören Druckereien, Lettershops, Callcenter, E-Mail-Dienstleister, Logistikunternehmen, Postdienstleister, Rechenzentren, Zahlungsdienstleister, Steuer- und Rechtsberater, Gewinnspieldienstleister und Analysedienstleister.

2. Wie sicher sind Ihre Daten?

Wir treffen geeignete technische und organisatorische Sicherheitsvorkehrungen, um Ihre personenbezogenen Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen und den Schutz Ihrer Rechte und die Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen der EU und der Bundesrepublik Deutschland zu gewährleisten.

Die ergriffenen Maßnahmen sollen die Vertraulichkeit und Integrität Ihrer Daten gewährleisten sowie die Verfügbarkeit und Belastbarkeit der Systeme und Dienste bei der Verarbeitung Ihrer Daten auf Dauer sicherstellen. Sie sollen außerdem die Verfügbarkeit der Daten und den Zugang zu Ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen.

Zu unseren Sicherheitsmaßnahmen gehört auch eine Verschlüsselung Ihrer Daten. Alle Informationen, die Sie online eingeben, werden technisch verschlüsselt und erst dann übermittelt. Dadurch können diese Informationen zu keinem Zeitpunkt von unbefugten Dritten eingesehen werden.

Unsere Datenverarbeitung und unsere Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

Unsere Mitarbeiter sind selbstverständlich schriftlich zur Vertraulichkeit verpflichtet (Datengeheimnis).

3. Unser Datenschutzbeauftragter

Wenn Sie eine Frage zum Datenschutz oder zur Datensicherheit haben, erreichen Sie unseren Datenschutzbeauftragten per E-Mail unter [datenschutz@faz.net](mailto:datenschutz@faz.net) oder per Post unter Frankfurter Allgemeine Zeitung GmbH, Abteilung Datenschutz, Hellerhofstraße 2-4, 60327 Frankfurt am Main.

4. Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Hierzu gehören Ihre Adressdaten, Telekommunikationsdaten, Registrierungsdaten, Bestelldaten, Anzeigedaten, Abonnementdaten, Finanzdaten und Bewerbungsdaten, aber auch Ihre IP-Adresse.

5. Was sind Pflichtangaben oder Pflichtfelder?

Wenn bei der Erhebung bestimmte Datenfelder als Pflichtfelder bezeichnet und/oder mit einem Sternchen ( \* ) gekennzeichnet sind, ist die Bereitstellung dieser Daten entweder gesetzlich oder vertraglich vorgeschrieben oder wir benötigen diese Daten für den Vertragsabschluss, die gewünschte Dienstleistung oder den angegebenen Zweck. Die Angabe der Daten liegt selbstverständlich auch bei den Pflichtfeldern in Ihrem Ermessen. Eine Nichtangabe kann zur Folge haben, dass der Vertrag von uns nicht erfüllt bzw. die gewünschte Dienstleistung nicht erbracht oder der angegebene Zweck nicht erreicht werden kann.

6. Wofür werden Ihre Daten verarbeitet?

a. Kontakt / Anfragen

Wenn Sie Fragen oder Wünsche haben, stehen wir Ihnen gerne zur Verfügung. Wir verarbeiten Ihre Angaben zur Beantwortung Ihrer Anfragen (Art. 6 Abs. 1 b, f DSGVO). Die Mitteilung von als Pflichtangaben gekennzeichneten Adress- und Telekommunikationsdaten ist dabei erforderlich, um Ihr Anliegen bearbeiten und beantworten zu können. Die freiwillige Angabe weiterer Daten erleichtert uns die Bearbeitung Ihrer Anfrage. Das Erbringen möglichst guter Leistungen für Sie, ist unser berechtigtes Interesse, soweit wir Ihre Daten auf dieser Rechtsgrundlage verarbeiten.

Die Angaben aus Ihrer Anfrage speichern wir nach Beantwortung der Anfrage im Regelfall für 1 Jahr für den Fall weiterer Nachfragen, falls es sich nicht um Handels- oder Geschäftsbriefe handelt; diese speichern wir nach den gesetzlichen Vorschriften für mindestens sechs Jahre (§ 257 Abs. 1 Nr. 2, Abs. 4 HGB, Art. 6 Abs. 1 c DSGVO).

b. Registrierung

Wir verarbeiten Ihre erforderlichen Registrierungsangaben (Pflichtangaben, z.B. Name, E-Mail-Adresse, Benutzername und Passwort) sowie die im Rahmen Ihrer Nutzung freiwillig mitgeteilten weiteren Daten (z.B. Ihre Abonnementnummer, Ihre Urlaubstermine und -adresse für unseren Urlaubsservice) für die jeweilige Einrichtung und Ihre Nutzung der Funktionen und Services unserer passwortgeschützten Bereiche (Art. 6 Abs. 1 b, f DSGVO). Das Erbringen möglichst guter Leistungen für Sie, ist unser berechtigtes Interesse, soweit wir Ihre Daten auf dieser Rechtsgrundlage verarbeiten.

Die Registrierungsangaben für Ihre Online-Konten speichern wir, bis Sie Ihr jeweiliges Online-Konto wieder aufheben, soweit keine andere Aufbewahrungszwecke entgegenstehen. Diese können sich z.B. aus Ihren Bestellungen/Anzeigen/Abonnements (s. Ziffer d.) oder aus Ihrer veröffentlichten Lesermeinung bzw. Ihrem veröffentlichten Kommentar ergeben (s. Ziffer c.).

Zur Verarbeitung Ihrer Registrierungsdaten für Zwecke der Vermeidung der missbräuchlichen Nutzung von Verbraucher-Abonnements bzw. zur internen Erlöszuordnung genutzter digitaler Produkte (s. Ziffer 10.).

c. Lesermeinungen / Kommentare / Briefe an die Herausgeber

Ihre Angaben in Ihren Lesermeinungen, Kommentaren und Briefen an die Herausgeber verarbeiten wir zur Veröffentlichung Ihrer Beiträge, um sich mit Themen öffentlich auseinander setzen zu können (Art. 6 Abs. 1 b, f DSGVO, journalistische Zwecke). Um Lesermeinungen bzw. Kommentare verfassen zu können, müssen Sie sich zunächst registrieren (siehe Ziffer b.). Um Briefe an die Herausgeber anzufertigen, müssen Sie uns Ihre erforderlichen Adress- und Telekommunikationsdaten mitteilen. Mit Lesermeinungen, Kommentaren und Briefen an die Herausgeber wird Ihr Name veröffentlicht. Sie können also nicht unter einem Pseudonym oder anonym publiziert werden. Das Erbringen möglichst guter Leistungen für Sie, ist unser berechtigtes Interesse, soweit wir Ihre Daten auf dieser Rechtsgrundlage verarbeiten.

Ihre Lesermeinungen, Kommentare und Briefe an die Herausgeber können online abgerufen werden, bis das entsprechende Thema nicht mehr aktuell bzw. relevant ist. Danach werden sie in unseren Archiven aufbewahrt.

d. Bestellungen, Anzeigen und Abonnements

Bei einer Bestellung, der Aufgabe einer Anzeige, einem Abonnement oder sonstigen vertragsbezogenen Anfragen verarbeiten wir Ihre personenbezogenen Daten zunächst zur Abwicklung der Bestellung bzw. des Abonnements, zur Schaltung der Anzeige und zur Rechnungsstellung (Art. 6 Abs. 1 b, f DSGVO). Soweit Daten als Pflichtangaben gekennzeichnet sind, sind sie für die Abwicklung des Vertrages bzw. zur Rechnungsstellung erforderlich. Für Bestellungen, Aufgaben von Anzeigen und Abonnements müssen Sie sich zunächst registrieren (s. Ziffer b.). Das Erbringen möglichst guter Leistungen für Sie, ist unser berechtigtes Interesse, soweit wir Ihre Daten auf dieser Rechtsgrundlage verarbeiten.

Ihre für die Bestellung, die Anzeige bzw. das Abonnement relevanten Daten und die dazu gehörigen Dokumente (z.B. Handelsbriefe, Rechnungen) speichern wir gemäß den gesetzlichen Anforderungen nach Abschluss des Vertrages nach den gesetzlichen Vorschriften für mindestens sechs Jahre bzw. zehn Jahre (§ 257 Abs. 4 HGB, § 147 Abs. 3 AO, Art. 6 Abs. 1 c DSGVO). Andere Daten werden spätestens nach einem Jahr gelöscht.

e. Bonitätsprüfung und Inkasso

Zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses können wir im Fall der Übernahme eines Zahlungsausfallrisikos bei der Auskunftei bei der Creditreform Frankfurt Emil Vogt KG, Börsenplatz 7-11, 60313 Frankfurt (Main) zur Wahrung unserer berechtigten Interessen an der Vermeidung von Zahlungsausfällen Bonitätsauskünfte einholen (Art. 6 Abs. 1 f DSGVO, § 31 BDSG). Hierzu übermitteln wir dieser Auskunftei die für eine Bonitätsauskunft benötigten personenbezogenen Daten und erhalten und verwenden anschließend einen Wahrscheinlichkeitswert über die Zahlungsfähigkeit bzw. Zahlungswilligkeit. Die Berechnung des Wahrscheinlichkeitswerts erfolgt dabei auf Basis wissenschaftlich anerkannter mathematisch-statistischer Verfahren. Dabei können auch Anschriftendaten genutzt werden. Ihre schutzwürdigen Belange werden gemäß den gesetzlichen Bestimmungen berücksichtigt. Die Bonitätsauskunft löschen wir nach unserer Entscheidung über die Begründung, Durchführung oder Beendigung des Vertragsverhältnisses.

Personenbezogene Daten über fällige unbezahlte und unbestrittene Forderungen können wir vier Wochen nach Zugang der ersten von insgesamt mind. zwei schriftlichen Mahnungen, bei der wir Sie über eine mögliche Berücksichtigung der Forderungsdaten durch Auskunfteien unterrichten, an die o.g. Auskunftei übermitteln, die diese Daten bei berechtigtem Interesse auch anderen Unternehmen zur Bonitätsprüfung zur Verfügung stellen (Art. 6 Abs. 1 f DSGVO, § 31 BDSG). Unter den gleichen Voraussetzungen können wir im Fall von unbezahlten Forderungen Ihre entsprechenden Daten der Creditreform Frankfurt Emil Vogt KG zum Einzug für uns (Inkasso) übermitteln.

f. Werbung

* Postwerbung und Kundenanalysen

Die Daten aus Bestellungen, Anzeigen, Abonnements, Gewinnspielen und sonstige außerhalb des Internets erhobene Daten verarbeiten wir für eigene Kundenanalysen und Postwerbung (Art. 6 Abs. 1 f DSGVO), um Ihnen möglichst passende Inhalte anbieten zu können. Unsere Analysen erfolgen regelmäßig pseudonymisiert.

* Telefonwerbung

Mit Ihrer jederzeitig widerruflichen, ausdrücklichen Einwilligung informieren wir Sie als Verbraucher per Telefon im Umfang Ihrer erteilten Einwilligung, nämlich regelmäßig zu Zwecken der eigenen Marktforschung, der Durchführung von Gewinnspielen und zur Werbung über unsere digitalen und gedruckten Verlagsprodukte (Zeitungen, Zeitschriften und Artikel) und Vorteile entsprechender Abonnements (Art. 6 Abs. 1 a DSGVO, § 7 Abs. 2 Nr. 2 Alt. 1 UWG). Ihre verpflichtenden Angaben bei Erteilung Ihrer Einwilligung verarbeiten wir, um Sie anrufen und persönlich ansprechen zu können.

Wenn Sie uns Ihre Einwilligung online erteilen, wird auch Ihre IP-Adresse erfasst und zu Dokumentationszwecken gespeichert (Art. 7 Abs. 1, Art. 6 Abs. 1 c DSGVO).

Unsere Geschäftskunden informieren wir auch telefonisch über unsere Vorteilsangebote, soweit wir annehmen dürfen, dass der Anzurufende nach den Umständen vor dem Anruf sowie nach Art und Inhalt der Werbung damit einverstanden ist (Art. 6 Abs. 1 f DSGVO, § 7 Abs. 2 Nr. 2 Alt. 2 UWG).

* E-Mail-Werbung

Mit Ihrer jederzeitig widerruflichen, ausdrücklichen Einwilligung informieren wir Sie per E-Mail im Umfang Ihrer erteilten Einwilligung, nämlich regelmäßig zu Zwecken der eigenen Marktforschung, der Durchführung von Gewinnspielen und zur Werbung über unsere digitalen und gedruckten Verlagsprodukte (Zeitungen, Zeitschriften und Artikel) und Vorteile entsprechender Abonnements (Art. 6 Abs. 1 a DSGVO, § 7 Abs. 2 Nr.3 UWG). Ihre verpflichtenden Angaben bei Erteilung Ihrer Einwilligung verarbeiten wir, um Ihnen die werbliche Nachricht zusenden und Sie persönlich ansprechen zu können.

Zur Einholung Ihrer Einwilligungen verwenden wir online das sog. Double-Opt-in-Verfahren, um zu vermeiden, dass unsere E-Mail-Nachrichten an E-Mail-Adressen von Personen versandt werden, die diese nicht angefordert haben. Hierbei wird nach den Vorgaben der Datenschutzaufsichtsbehörden auch Ihre IP-Adresse erfasst und zu Dokumentationszwecken gespeichert (Art. 7 Abs. 1, Art. 6 Abs. 1 c DSGVO).

Wenn Sie uns bei Ihrem Vertragsschluss (z.B. bei Bestellungen, Anzeigen, Abonnements oder sonstigen Austauschverträgen) Ihre E-Mail-Adresse mitgeteilt haben, informieren wir Sie auch per E-Mail über Angebote, die den von Ihnen gekauften bzw. erhaltenen ähnlich sind. Dem können Sie selbstverständlich jederzeit zu Basistarifen widersprechen (Art. 6 Abs. 1 f DSGVO, § 7 Abs. 3 UWG).

* Gewinnspiele und Verkaufsförderungsmaßnahmen

Wenn Sie an unseren Gewinnspielen oder Verkaufsförderungsmaßnahmen teilnehmen, verarbeiten wir und unsere jeweiligen Kooperationspartner (z.B. Preissponsoren) Ihre Daten zur Durchführung des Gewinnspiels oder der Verkaufsförderungsmaßnahme (Art. 6 Abs. 1 b DSGVO). Wir und ggf. auch unsere jeweiligen Kooperationspartner verarbeiten Ihre Daten auch für jeweils eigene Kundenanalysen und jeweils eigene Werbung per Post (s. Abs. Postwerbung und Kundenanalysen). Für bestimmte Gewinnspiele müssen Sie sich zunächst registrieren. Näheres zum FAZ.NET-Orakel unter Ziffer 11.

* Speicherdauer bei Werbung

Ihre für Werbezwecke erhobenen Daten speichern wir solange der Werbezweck besteht bzw. bis uns ein Widerruf Ihrer Einwilligung oder Ihr Widerspruch gegen die Verarbeitung Ihrer Daten für Werbezwecke erreicht (s. Ziffer 7.). Soweit für vorstehende Zwecke nicht erforderlich, löschen wir Daten aus Ihrer Teilnahme an Gewinnspielen oder Verkaufsförderungsmaßnahmen nach Durchführung des jeweiligen Gewinnspiels bzw. der jeweiligen Verkaufsförderungsmaßnahmen, es sei denn wir sind zur Aufbewahrung verpflichtet (z.B. im Falle eines Gewinns werden Handels- bzw. Geschäftsbriefe für 10 Jahre aufbewahrt, § 147 AO, § 257 HGB).

* Zweckänderung

Sollten wir die Zwecke der Verarbeitung im Laufe der Zeit ändern, werden wir Sie durch eine Aktualisierung dieser Hinweise zum Datenschutz vorab informieren.

g. Visitenkarten

Wir verarbeiten Ihre Kontaktdaten aus von Ihnen erhaltenen Visitenkarten für die weitere Kontaktaufnahme für Ihnen mitgeteilte Zwecke und über mit Ihnen abgestimmte Adressen (Art. 6 Abs. 1 a DSGVO). Die Kontaktdaten benötigen wir, wenn wir Sie entsprechend kontaktieren sollen. Ihre Einwilligung können Sie jederzeit für die Zukunft widerrufen.

Ihre Daten speichern wir solange der vorstehende Zweck besteht bzw. bis uns ein Widerruf Ihrer Einwilligung oder Ihr Widerspruch gegen die Verarbeitung Ihrer Daten erreicht (s. Ziffer 7.).

h. Umfragen

Wir verarbeiten Ihre in Umfragen mitgeteilten Daten für die Abwicklung und Auswertung der Umfrage, deren Zwecke jeweils bei der Umfrage angegeben sind (Art. 6 Abs. 1 b, f DSGVO). Die Pflichtangaben benötigen wir, um plausible Ergebnisse zu generieren. Ihre Daten speichern wir, solange sie für vorgenannte Zwecke erforderlich sind, das bedeutet meist nicht länger als sechs Monate. Das Erzielen möglichst plausibler Umfrage-Ergebnisse, ist unser berechtigtes Interesse, soweit wir Ihre Daten auf dieser Rechtsgrundlage verarbeiten. Zur Einbindung von Umfragen über externe Dienste beachten Sie bitte Ziffer 11.

i. Redaktionelle Nachrichten

* FAZ-Newsletter

Mit Ihrer jeweils jederzeitig widerruflichen, ausdrücklichen Einwilligung informieren wir Sie per E-Mail mit unseren verschiedenen redaktionellen FAZ-Newslettern (Art. 6 Abs. 1 a DSGVO). Ihre verpflichtenden Angaben bei Erteilung Ihrer Einwilligung verarbeiten wir, um Ihnen den/die von Ihnen gewählten Newsletter zusenden und Sie persönlich ansprechen zu können.

Zur Einholung Ihrer Einwilligungen verwenden wir online das sog. Double-Opt-in-Verfahren, um zu vermeiden, dass unsere E-Mail-Nachrichten an E-Mail-Adressen von Personen versandt werden, die diese nicht angefordert haben. Hierbei wird nach den Vorgaben der Datenschutzaufsichtsbehörden auch Ihre IP-Adresse erfasst und zu Dokumentationszwecken gespeichert (Art. 7 Abs. 1, Art. 6 Abs. 1 c DSGVO).

* Web-Push-Nachrichten

Mit Ihrer jederzeitig widerruflichen, ausdrücklichen Einwilligung informieren wir Sie mit Web-Push-Benachrichtigungen (Art. 6 Abs. 1 a DSGVO). Bei Web-Push-Benachrichtigungen handelt es sich um regelmäßige Informationen zu den wichtigsten Ereignissen des Tages, die mithilfe unseres beauftragten Push-Dienstleisters an Ihren Browser bzw. Ihr Endgerät gesendet und dort priorisiert (in der Regel im Header des Browsers) dargestellt werden.

Um sich für die Web-Push-Nachrichten anzumelden („Einwilligung"), müssen Sie den Hinweis Ihres Browsers zu Web-Push-Benachrichtigungen mit einem Klick auf den Button „Zulassen“ bestätigen. Der Hinweis wird angezeigt, wenn Sie auf unserer Webseite navigieren (in der Regel im Header des Browsers). Um Ihre Anmeldung nachzuvollziehen bzw. zu dokumentieren (Art. 7 Abs. 1, Art. 6 Abs. 1 c DSGVO) und Ihnen Nachrichten senden zu können, werden unter anderem der Anmeldezeitpunkt, Angaben zum Browser sowie ein sog. Push-Token bzw. eine Geräte-ID (Gerätekennzeichen) gespeichert. Der Push-Token verhält sich wie ein Endpunkt zum Versenden der Push-Nachricht an den richtigen Browser, ähnlich der Geräte-ID, welche den Endpunkt bei Smartphones darstellt und das empfangende Gerät identifiziert.

Um Inhalte unserer Nachrichten zu verbessern, passender auf die Interessen von unseren Lesern auszurichten und die Funktionalität der Nachrichten sicherzustellen, kann unser Push-Dienstleister nachvollziehen, ob und wann welche Nachrichten zugestellt und geöffnet wurden (Art. 6 Abs.1 f DSGVO). Wir erhalten für vorstehende Auswertungszwecke anonyme Statistiken.

Ihre Einwilligung in die Verarbeitung Ihrer Daten zum Erhalt unserer Push-Benachrichtigungen können Sie jederzeit mit Wirkung für die Zukunft in den Einstellungen Ihres Browsers oder unter folgendem Link widerrufen:

<https://www.faz.net/?cleverPushUnsubscribe=true>

Weitere Datenschutz-Informationen zu Web-Push-Benachrichtigungen und wie Sie diese deaktivieren können, finden Sie hier: <https://www.faz.net/hilfe/web-push-die-wichtigsten-news-per-push-benachrichtigung-faz-16754999.html> und <https://cleverpush.com/faq>.

j. Verlängerte Speicherfristen

Die angegebenen Speicherfristen können sich entsprechend verlängern, wenn im Einzelfall, insbesondere wenn die Daten für verschiedene Zwecke verarbeitet werden, eine längere gesetzliche oder vertragliche Aufbewahrungsfrist besteht.

7. Jederzeitiges Widerspruchs- und Widerrufsrecht

Sie haben das Recht, jederzeit aus Gründen, die sich aus Ihrer besonderen Situation ergeben, bei Vorliegen der gesetzlichen Voraussetzungen gegen die Verarbeitung Ihrer Daten Widerspruch einzulegen.

Wenn Sie der Verarbeitung Ihrer Daten für Werbezwecke widersprechen oder eine erteilte Einwilligung widerrufen möchten, genügt jederzeit eine kurze Nachricht an unseren Datenschutzbeauftragen per E-Mail an [datenschutz@faz.net](mailto:datenschutz@faz.net) oder per Post an Frankfurter Allgemeine Zeitung GmbH, Abteilung Datenschutz, Hellerhofstraße 2-4, 60327 Frankfurt am Main. Ihre Daten werden dann nicht mehr für die vom Werbewiderspruch oder dem Widerruf der Einwilligung erfassten Zwecke der Werbung verarbeitet.

Die Rechtmäßigkeit der bis zum Widerspruch bzw. Widerruf erfolgten Verarbeitung bleibt dadurch unberührt.

Nach Ihrem Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten für Werbezwecke bzw. dem Widerruf Ihrer Einwilligung sind wir datenschutzrechtlich nach den Vorgaben der deutschen Datenschutzaufsichtsbehörden verpflichtet, die hierfür erforderlichen Daten (Name, Anschrift, E-Mail-Adresse) in unsere interne Werbesperrliste aufzunehmen und dauerhaft – nur für diesen Zweck – zu speichern (zu sperren) und zum Abgleich mit unseren künftigen Werbedateien zu verwenden (Art. 21 Abs. 3, Art. 17 Abs. 3 b, Art. 6 Abs. 1 c DSGVO). So lässt sich die Beachtung Ihres Werbewiderspruchs bzw. des Widerrufs Ihrer Einwilligung dauerhaft sicherstellen.

8. Cookies und andere Technologien

a. Einsatz durch uns und unsere Partner

In bestimmten Fällen benötigen wir Ihre Zustimmung zur Verwendung von Cookies und anderen Technologien durch uns (Frankfurter Allgemeine Zeitung GmbH) und unsere Partner, um persönliche Daten auf Ihrem Gerät zu speichern und abzurufen (§ 15 TMG, Art. 6 Abs. 1 a DSGVO).

In einigen Fällen verarbeiten wir und einige unserer Partner Ihre persönlichen Daten außerdem auf Grundlage von berechtigtem Interesse (Art. 6 Abs. 1 f DSGVO). Dabei können ebenso Cookies und andere Technologien eingesetzt werden. Berechtigte Interessen sind die Werbefinanzierung des Online-Auftritts, die Zurverfügungstellung möglichst passender Inhalte für unsere Leser und/oder technische oder gesetzliche Erfordernisse. Zu technischen Erfordernissen zählen: Sicherheit gewährleisten, Betrug verhindern und Fehler beheben, Anzeigen oder Inhalte technisch bereitstellen, notwendige Technologien. Im Übrigen können Einbindung von Inhalten, die auf anderen Servern gehostet werden, Reichweitenmessung und statistische Analysen, Optimierung des jeweiligen Webangebots sowie  
Wiedererkennung und Merkmalszuordnung der Nutzer, z.B. bei werbefinanzierten Angeboten genannt werden.

Grundsätzlich werden folgende Zwecke verfolgt, zu denen Sie im Einzelnen in unserem [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html)nachlesen können:

Personalisierte Inhalte auswählen; Personalisierte Anzeigen auswählen; Auswahl einfacher Anzeigen; Ein personalisiertes Anzeigen-Profil erstellen; Ein personalisiertes Inhalts-Profil erstellen; Anzeigen-Leistung messen; Inhalte-Leistung messen, Marktforschung einsetzen, um Erkenntnisse über Zielgruppen zu gewinnen; Produkte entwickeln und verbessern; Einbindung von externen Multimedia-Inhalten; Sicherheit gewährleisten, Betrug verhindern und Fehler beheben; Anzeigen und Inhalte technisch bereitstellen; Notwendige Technologien einsetzen.

Hierzu werden auch folgende Funktionen eingesetzt: Personalisierte Inhalte auswählen; Zusammenführen mit Offline-Datenquellen; Verschiedene Funktionen verknüpfen; Empfangen und Verwenden automatisch gesendeter Geräteeigenschaften für die Identifikation.

Im [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html) können Sie u.a. zu Partnern und Cookies nachlesen, aber auch vor allem Ihre Zustimmung im von Ihnen gewünschten Umfang erteilen und widerrufen. Widerspruchsmöglichkeiten sind vorgesehen, soweit dem keine technischen Gründe entgegenstehen.

Bei „persönlichen Daten“ handelt es sich um bestimmte Informationen, zu denen Sie im [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html) nachlesen können und zu denen auch IP-, ID- und Browserinformationen zählen können.

Der [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html) wird uns durch einen beauftragten IT-Dienstleister zur Verfügung gestellt, der hierzu entsprechend Zugriff auf Ihre Daten nehmen kann.

Soweit Sie Ihre Zustimmung erteilen bzw. ein berechtigtes Interesse vorliegt, gilt diese/s für uns und unsere Partner für unsere Stamm-Domäne faz.net, aber auch hinsichtlich hier einsehbarer faz.net-Seiten und jeweilige Unterseiten. Ihre Zustimmung beinhaltet auch die Verarbeitung der Daten außerhalb des Europäischen Wirtschaftsraumes (Art. 49 Abs.1 a DSGVO), wo unter Umständen kein vergleichbares Datenschutzniveau herrscht, z.B. in den USA. Hinsichtlich den USA besteht insbesondere das Risiko, dass Ihre Daten durch US-Behörden zu Überwachungszwecken verarbeitet werden, möglicherweise auch ohne Durchsetzbarkeit Ihrer Rechte und entsprechende Rechtsbehelfsmöglichkeiten. Beachten Sie bitte im Übrigen unten Ziffer 8.c.(2) zu von Dritten betriebenen faz.net-Seiten.

Ihre vorgenommenen Einstellungen im [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html) (z.B. Umfang Ihrer Zustimmung) wird mit einem Cookie zur technischen Dokumentation ebenso auf Ihrem Endgerät zum Abruf hinterlegt.

b. Individuelle Cookie-Einstellungen über Ihren Browser

Neben der Steuerung der einsetzbaren Cookies und anderen Techniken in unserem [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html), haben Sie auch allgemein die Möglichkeit, Cookie-Einstellungen über Ihren Webbrowser vorzunehmen. Sie können Ihren Webbrowser so einstellen, dass er Sie beim Setzen von Cookies benachrichtigt oder Cookies generell ablehnt. Wenn Sie den Einsatz von Cookies mithilfe Ihres Browsers deaktivieren bzw. einschränken, werden jedoch verschiedene Funktionen auf unserer Website für Sie nicht mehr nutzbar sein. Sie können Cookies löschen, auch automatisiert. Das Löschen von Cookies löscht auch eine ggfs. erteilte Zustimmung (dazu soeben Ziffer 8.a.).

Über die folgenden Links können Sie sich über die Möglichkeit, individuelle Cookie-Einstellungen über Ihren Browser vorzunehmen, für die am meisten verwendeten Browser informieren:

* Internet Explorer: <https://support.microsoft.com/de-de/help/17442/windows-internet-explorer-delete-manage-cookies>
* Firefox: <http://support.mozilla.org/de/kb/cookies-informationen-websites-auf-ihrem-computer>
* Google Chrome: <http://support.google.com/chrome/bin/answer.py?hl=de&answer=95647>
* Safari: <https://support.apple.com/de-de/guide/safari/sfri11471/mac>
* Opera: <https://help.opera.com/de/latest/web-preferences/>

c. Darstellung von FAZ-Inhalten auf Seiten Dritter

(1) Accelerated Mobile Page

Wenn Sie unsere Artikel über die Google Suche (erkennbar am kleinen grauen Blitz) oder in Apps sozialer Medien wie z.B. Linkedin oder Twitter aufrufen, wird Ihnen in einigen Fällen die sog. „Accelerated Mobile Page“ Variante unseres Artikels angezeigt, um mobile Websites schneller und besser nutzen zu können. Sie lesen den Artikel dann auf einer Plattform von Google, auf die wir keinen Einfluss haben. Vielmehr stellen wir Google nur unseren Inhalt zur Verfügung. Sie merken dies z.B. daran, dass in der URL, auf der Sie den Artikel lesen, nicht unser Domainname (also unsere Internetadresse), sondern der Domainname von Google (z.B. [google.de](http://google.de/)) angezeigt wird. Bitte beachten Sie, dass in diesen Fällen Einstellungen über unseren Cookie-Manager nicht funktionieren. Wählen Sie bitte die Alternative mit Ihren Browsereinstellungen (b.), um Cookie-Einstellungen zu ändern. Nähere Informationen zu Zweck und Umfang der möglichen Datenverarbeitung durch Google und Ihre diesbezüglichen Einstellungsmöglichkeiten zum Schutz Ihrer Privatsphäre finden Sie unter <https://policies.google.com/privacy?hl=de>.

(2) Von Dritten betriebene faz.net-Seiten

Einige unserer faz.net-Seiten werden von Dritten betrieben. Teilweise agieren die Betreiber dabei als datenschutzrechtlich eigene Verantwortliche. Soweit diese dann eigenständig Cookies und andere Techniken einsetzen, sind wir dafür nicht verantwortlich. Insbesondere gelten Ihre uns und unseren Partnern erteilte Zustimmung bzw. ein durch uns mitgeteiltes berechtigtes Interesse und entsprechende Datenverarbeitungen (s. oben Ziffer 8.a. bzw. unser [Cookie-Manager](https://www.faz.net/datenschutzerklaerung-11228151.html)) dann auch nicht für diese Dritte. Bitte informieren Sie sich in den jeweiligen Datenschutzinformationen der Seiten.

9. Soziale Medien

a. Nachrichtenversand über WhatsApp, Telegram, Facebook Messenger und Notify

Mit Ihrer jederzeitig widerruflichen Einwilligung informieren wir Sie via WhatsApp, Facebook Messenger, Telegram, Apple Business Chat und/oder Notify mit Hilfe unseres beauftragten Dienstleisters, der MessengerPeople GmbH, Herzog-Heinrich-Str. 9, 80336 München, Deutschland, per entsprechender Nachricht über bestimmte Themen. Sie erhalten von uns im gewählten Service eine Nachricht am frühen Abend mit einer kompakten Übersicht zu den wichtigsten Themen des Tages sowie allgemein die wichtigsten Eilmeldungen (Art. 6 Abs. 1 a DSGVO, § 7 Abs. 2 Nr. 3 UWG).

Um diese Nachrichten zu erhalten, können Sie auf einigen Seiten unseres Online-Angebotes in der dafür vorgesehenen Informations-Box zunächst per Klick den Service auswählen, den Sie nutzen möchten (WhatsApp, Facebook Messenger und/oder Telegram, Apple Business Chat, Notify).

Für die Nutzung des WhatsApp-Service müssen Sie sodann den weiteren Anweisungen in der Informations-Box folgen, u.a. die angezeigte Rufnummer als Kontakt in Ihrem Smartphone anlegen, und uns schließlich eine Nachricht per WhatsApp mit dem Wort „Start“ senden (ohne Anführungszeichen). Damit startet der WhatsApp-Service.

Für die Nutzung des Facebook Messenger-Service müssen Sie den weiteren Anweisungen in der Informations-Box folgen und auf den Facebook Messenger-Button in der Informations-Box klicken. Dadurch werden Sie zum Facebook Messenger weitergeleitet.    
Alternativ rufen Sie unsere Facebook-Seite unter <https://www.facebook.com/faz/> auf und klicken auf den „Nachricht“-Button rechts unter dem Titelbild, wodurch sich ebenso der Facebook Messenger öffnet. Folgen Sie in allen Fällen den weiteren Anweisungen und klicken Sie im Chatfenster auf „Los geht‘s“ bzw. - falls kein Button angezeigt wird -senden Sie das Wort „Start“ (ohne Anführungszeichen). Damit startet der Facebook Messenger-Service.

Für die Nutzung des Telegram-Service müssen Sie ebenso den weiteren Anweisungen in der Informations-Box folgen, u.a. unseren Kontakt FAZ\_NET\_Bot in der Telegram-App suchen und auswählen. Klicken Sie im Chatfenster schließlich auf „Start“. Damit startet der Telegram-Service.

Für die Nutzung des Notify-Service müssen Sie in der Notify-App unter “Entdecken“ unseren Kanal “FAZ“ suchen, anklicken und bei “Abonnieren“ den Slider-Button aktivieren.

Für die Nutzung des Apple Business Chat-Service müssen Sie den weiteren Anweisungen in der Informationsbox folgen und anschließend eine Nachricht mit dem Wort “Start” (ohne Anführungszeichen) in unseren Kanal schreiben. Sie werden dann gefragt, ob sie unsere Nachrichten erhalten wollen und müssen noch einmal bestätigen.

Wir und unser beauftragter Dienstleister verarbeiten Ihre Telefonnummer, Ihre E-Mailadresse, Ihr Nutzungsgerät, ggf. eine Messenger-ID, Informationen über die von Ihnen gelesenen Nachrichten, die Chathistorie, Ihren Profilnamen, Ihr Profilfoto und eventuell andere Profildaten sowie in allen Fällen Informationen zur Erteilung Ihrer Einwilligung, jeweils für die Erbringung des Messenger-Service.

Wenn Sie keine Nachrichten mehr erhalten wollen, senden Sie im jeweiligen Nachrichtendienst den Befehl „Stop“ (ohne Anführungszeichen) an uns. Damit haben Sie Ihre Einwilligung widerrufen. Dann erhalten Sie in der Zukunft keine Nachrichten über den jeweiligen Service von uns, bis Sie im jeweiligen Service wieder "Start" an uns schicken (ohne Anführungszeichen).

Wenn Sie im jeweiligen Service „ALLE DATEN LOESCHEN“ senden (ohne Anführungszeichen), werden die bei uns bzw. unserem Dienstleister hinterlegten Daten gelöscht. Die Löschung aus den Backupdaten unseres Dienstleisters erfolgt innerhalb von 61 Tagen.

Weitere Informationen zu Zweck und Umfang der Datenverarbeitung durch WhatsApp (WhatsApp Inc., 1601 Willow Road, Menlo Park, California 94025, USA) und Ihre diesbezüglichen Einstellungsmöglichkeiten finden Sie unter <https://www.whatsapp.com/legal/#privacy-policy>.

Weitere Informationen zur Datenverarbeitung von Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland (Muttergesellschaft: Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA) und zu Einstellungsmöglichkeiten zum Schutz Ihrer Privatsphäre finden Sie unter <http://www.facebook.com/about/privacy/>.

Weitere Informationen zu Zweck und Umfang der Datenverarbeitung durch Telegram (71-75 Shelton Street, Covent Garden, London, United Kingdom) und Ihre diesbezüglichen Einstellungsmöglichkeiten finden Sie unter <https://telegram.org/privacy>.

Weitere Informationen zu Zweck und Umfang der Datenverarbeitung durch Notify (MessengerPeople GmbH, Herzog-Heinrich-Str. 9, 80336 München, Deutschland) finden Sie unter <https://www.messengerpeople.com/de/notify-datenschutzerklaerung/>.

Weitere Informationen zu Zweck und Umfang der Datenverarbeitung durch Apple (Apple Inc., Infinite Loop, Cupertino, CA 95014) finden Sie unter <https://support.apple.com/en-euro/HT210666>.

Eine ausführliche Datenschutzerklärung unseres Dienstleisters MessengerPeople GmbH finden Sie unter <https://www.messengerpeople.com/de/datenschutzerklaerung/>.

b. Facebook-, Instagram- und Youtube-Kommentarprüfung durch ferret go GmbH

Die ferret go GmbH, Brauerstraße 14, 16321 Bernau bei Berlin, verarbeitet in unserem Auftrag veröffentlichte Kommentare, welche von Facebook Nutzern auf unseren Facebook Pages, von Youtube Nutzern auf unseren Youtube Kanälen, oder von Instagram Nutzern auf unseren Instagram Accounts abgegeben werden, hinsichtlich der Einhaltung der von uns vorgegebenen Netiquette-Regeln oder auf strafrechtlich relevante Aussagen, um unsere Rechte zu schützen (Art.6 Abs.1 b, f DSGVO). Dabei werden im Falle der Facebook-Kommentarprüfung die Facebook-Nutzer-ID, der Kommentartext sowie Datum und Uhrzeit des Kommentars verarbeitet. Bei der Instagram-Kommentarprüfung werden der Nutzername bzw. die Nutzer-ID, der Kommentartext sowie Datum und Uhrzeit des Kommentars verarbeitet. Bei der Youtube-Kommentarprüfung werden zum Beispiel Nachricht, Erstellungsdatum, Updatedatum, Kanal-ID, Autor-Profile URL, Autor Image URL, auf Kommentare/Posts assoziierte Daten wie Name/Nutzername, eindeutige Nutzer-ID, Meta-Daten wie beispielsweise Kommentare/Posts und Inhalte, Datum, Zeit, Stimmung und Nutzerbewertung verarbeitet.

Soweit keine Verstöße festgestellt werden, werden die verarbeiteten Daten umgehend wieder gelöscht. Ansonsten behalten wir uns eine Weitergabe der Daten an Strafverfolgungsbehörden und die längere Verarbeitung der Daten zum Ausschluss des jeweiligen Nutzers von der Kommentarfunktion vor.

Eine ausführliche Datenschutzerklärung unseres Dienstleisters ferret go GmbH finden Sie unter <https://www.conversar.io/de/datenschutz>.

10. Datenbank zur Verhinderung missbräuchlicher Nutzung / Erlöszuordnung

Bestimmte Abonnements dürfen entsprechend der vertraglichen Vereinbarungen nur von Verbrauchern genutzt werden. Um eine missbräuchliche Nutzung dieser Abonnements über die vertraglich vereinbarten Zwecke hinaus erkennen und ggf. reagieren zu können, werden bei der Nutzung des entsprechenden Abonnements mithilfe der Techniken von AT Internet, auch unter Einsatz von Cookies bzw. ähnlicher Technologien (s. Ziffer 8.) generierte Daten (Datum und Uhrzeit der Nutzung, digitales F.A.Z.-Produkt, Kunden-ID. Login aus der Online-Registrierung) in unserer internen Datenbank zum Schutz unserer Rechte verarbeitet (Art.6 Abs.1 b, f DSGVO). Ebenso werden bei der Nutzung digitaler F.A.Z.-Produkte (z.B.  F.A.Z. Digitale Zeitung) solche Daten in einer Datenbank verarbeitet, um die interne Zuordnung von Erlösen zu den genutzten digitalen F.A.Z.-Produkten bestimmen zu können und damit auch unsere Produkte bewerten zu können (Art.6 Abs.1 f DSGVO). Die Daten werden gelöscht bzw. anonymisiert, sobald deren personenbezogene Verarbeitung für die vorstehenden Zwecke nicht mehr erforderlich ist.

11. Fremde Inhalte und Dienste von Dienstleistern

a. VWD Musterdepot / Börsenspiel

(1) Die F.A.Z. bietet zusammen mit dem Dienstleister VWD Vereinigte Wirtschaftsdienste GmbH (Mainzer Landstraße 178 – 190, 60327 Frankfurt am Main) ein Musterdepot und ein Börsenspiel an. In beiden Tools hat der Nutzer die Möglichkeit, mit virtuellem Kapital Wertpapiere zu kaufen und zu verkaufen. Um diese Tools nutzen zu können, muss der Nutzer auf FAZ.NET eingeloggt sein. Die F.A.Z. stellt der VWD die E-Mail-Adresse und den Benutzernamen der Nutzer, die diesen Dienst nutzen, zur Verfügung, um den Dienst anbieten zu können (Art. 6 Abs. 1 f DSGVO). Zudem speichert die VWD beim Kauf/Verkauf von Wertpapieren folgende Daten: das virtuelle Kapital, die Daten der virtuellen Transaktion (Kaufdatum, Wertpapier, Anzahl, Kaufkurs, Währungskurs, Währung, Börse, Spesen).

Hat ein Nutzer einen die E-Mail-Benachrichtigung (die sich wahlweise täglich, monatlich oder wöchentlich zu einem bestimmten Wochentag einstellen lässt) für sein Musterdepot aktiviert, versendet die VWD E-Mails an die E-Mail-Adresse des Nutzers in dem gewünschten Rhythmus.

Die Daten werden gelöscht, sobald der Nutzer mitteilt, dass er nicht mehr den jeweiligen Dienst nutzen möchte oder aber sein FAZ-Konto löscht (s. Ziffer 6.b.), es sei denn es stehen anderweitige Aufbewahrungspflichten entgegen.

(2) Dergleichen bietet die F.A.Z. mit Unterstützung des Karlsruher Instituts für Technologie (Kaiserstr. 12, 76131 Karlsruhe, „KIT“) eine Prognosebörse an. Der Nutzer hat dabei die Möglichkeit Aktien bezüglich zukünftigen Ereignissen zu handeln. Um das Tool nutzen zu können bzw. am Spiel teilnehmen zu können (Teilnahmebedingungen [hier](https://orakel.faz.net/home/terms) abrufbar), muss der Nutzer auf FAZ.NET eingeloggt sein (zur Registrierung s. oben Ziffer 6.b.). Die F.A.Z. stellt dem KIT die E-Mail-Adresse, den Benutzernamen, Namen sowie Vornamen der Nutzer, die die Prognosebörse  nutzen, zur Verfügung, um den Dienst mit anbieten und Gewinner per E-Mail benachrichtigen zu können. Der Nutzer wird mit seinem Benutzernamen in einer Rangliste geführt, Gewinner werden mit ihrem Namen und Vornamen auf unserer Website veröffentlicht. Preissponsoren können für die Übergabe des Gewinns Gewinnerdaten (Name, Anschrift, E-Mail-Adresse) erhalten (Art. 6 Abs. 1 b, f DSGVO).

Hat ein Nutzer die E-Mail-Benachrichtigung für seine Prognosebörse aktiviert, versendet das KIT jederzeit für die Zukunft widerruflich E-Mails an die E-Mail- Adresse des Nutzers, um über neue Märkte oder administrative Änderungen zu informieren (Art. 6 Abs.1 a DSGVO). Der Versand der E-Mails kann an entsprechender Stelle wieder deaktiviert werden.

Die Daten werden gelöscht, sobald der Nutzer mitteilt, dass er nicht mehr am Spiel teilnehmen möchte oder sein FAZ-Konto löscht (s. Ziffer 6.b.), es sei denn es stehen anderweitige Aufbewahrungspflichten entgegen.

b. Einbindung fremder Inhalte

Auf unseren Websites werden fremde Inhalte eingebettet, um Ihnen bestimmte Funktionen anbieten zu können, z.B. Vergleichsrechner, Wetterseiten, TV-Programme, Senioreneinrichtungs-Informationen, Videoplayer, Veranstaltungskalender, Börsenkurse, Börsenlexika oder Spiele. Die Inhalte werden uns jeweils durch unsere entsprechenden Dienstleister zur Verfügung gestellt. Diese Inhalte sind regelmäßig mittels JavaScript bzw. Framing oder anderen technischen Lösungen auf unserer Webseite eingebunden und durch Angabe des jeweiligen Dienstleisters kenntlich gemacht. Wenn Sie eine Unterseite aufrufen, die einen solchen fremden Inhalt enthält, wird Ihre IP-Adresse bzw. Angaben zu Ihrem Endgerät an unseren jeweiligen Dienstleister zur Ermöglichung der Darstellung des Inhalts bzw. der Funktion und ggf. zur internen Abrechnung zwischen dem Dienstleister und uns übermittelt. Dies geschieht je nach Konstellation auf Basis des berechtigten Interesses (Art. 6 Abs. 1 f DSGVO) oder auf Grundlage einer Auftragsverarbeitung (Art. 28 DSGVO). Etwaige personenbezogene Daten, die Sie darüber hinaus hierbei eingeben, werden für Zwecke des angeforderten Inhalts bzw. der Bearbeitung Ihrer Eingabe durch den Dienstleister verarbeitet. Es können auch Cookies oder ähnliche Techniken von uns oder unseren Dienstleistern eingesetzt werden (s. Ziffer 8.).

c. Umfragen zu unseren digitalen Produkten auf externen Seiten

Wir führen mithilfe des Tools SurveyMonkey, einem Angebot unseres Dienstleisters SurveyMonkey Europe UC, 2 Shelbourne Buildings, Shelbourne Road, Dublin, Ireland („SurveyMonkey“; Muttergesellschaft: SurveyMonkey Inc, USA), Umfragen zu unseren digitalen Produkten durch. Diese Umfragen erfolgen mit unserem Interesse die Qualität unserer Produkte weiter zu verbessern (Art. 6 Abs. 1 f DSGVO). Unser Interesse an der Einbindung unseres Dienstleisters bei der Verarbeitung liegt im arbeitsteiligen Wirtschaften.

Um an diesen Umfragen teilzunehmen, müssen Sie auf einen Link klicken, der in unseren Webseiten, Apps bzw. über ein Banner angezeigt wird. Durch das aktive Anklicken des Links werden Sie auf eine externe Webseite von SurveyMonkey weitergeleitet, auf der die Umfrage stattfindet.

Auf der externen Webseite erfasst SurveyMonkey für uns Ihre mitgeteilten Umfragedaten rund um die Nutzung und Verwendung unserer digitalen Produkte durch Sie. SurveyMonkey erfasst diese Umfragedaten nur, um sie an uns weiterzuleiten. Wie wir Ihre mitgeteilten Umfragedaten verarbeiten, können Sie in Ziffer 6.h. (Umfragen) nachlesen.

Außerdem verarbeitet SurveyMonkey Informationen über Ihr Endgerät und die App, das bzw. die der Nutzer für seine Teilnahme an der Umfrage einsetzt. Dazu gehört die IP-Adresse, die Version des Betriebssystems, der Gerätetyp, die Geräte-ID/MAC-Adresse sowie der Browsertyp. Wenn Sie ein Mobilgerät einsetzen, erfasst SurveyMonkey zusätzlich die UUID dieses Geräts. SurveyMonkey benutzt zudem Cookies und Tracking Services von Erst- und Drittanbietern zur Webanalyse, um Nutzungsdaten und Anwenderstatistiken zu erfassen. Diese werden auf den Webseiten, auf denen die Umfragen zur Verfügung gestellt werden, und in den von der F.A.Z. versendeten Umfrage-Mails eingesetzt.

Nähere Informationen zu Zweck und Umfang der Datenverarbeitung durch SurveyMonkey finden Sie unter [https://www.surveymonkey.de/mp/legal/privacy-policy.](https://www.surveymonkey.de/mp/legal/privacy-policy/)

Den Einsatz von Cookies können Sie mithilfe Ihres Browsers deaktivieren bzw. einschränken, weitere Informationen dazu finden Sie unter Ziffer 8.b.

Es ist nicht ausgeschlossen, dass die durch SurveyMonkey erhobenen Daten auch in die USA übermittelt werden, in dem aktuell kein vergleichbares Datenschutzniveau vorherrscht.

12. Wie können Sie Ihre Datenschutzrechte wahrnehmen?

Wenn Sie Fragen zu der Verarbeitung Ihrer personenbezogenen Daten durch uns haben, erteilen wir Ihnen selbstverständlich gerne Auskunft über die Sie betreffenden Daten (Art. 15 DSGVO).

Außerdem haben Sie bei Vorliegen der gesetzlichen Voraussetzungen ein Recht auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO), Widerspruch (Art. 21 DSGVO, dazu oben Ziffer 7.) und Datenübertragbarkeit (Art. 20 DSGVO).

Bitte wenden Sie sich in all diesen Fällen gerne an unseren Datenschutzbeauftragten (s. Ziffer 3.) unter den dort genannten Kommunikationsadressen.

Schließlich haben Sie das Recht auf Beschwerde bei einer zuständigen Datenschutz-Aufsichtsbehörde (Art. 77 DSGVO, § 19 BDSG).

13. Änderungen

Von Zeit zu Zeit ist es erforderlich, den Inhalt der vorliegenden Hinweise zum Datenschutz anzupassen. Wir behalten uns daher vor, diese jederzeit für die Zukunft zu ändern. Wir werden die geänderte Version der Datenschutzhinweise ebenfalls an dieser Stelle veröffentlichen. Wenn Sie uns wieder besuchen, sollten Sie sich daher die Datenschutzhinweise erneut durchlesen.

Stand: Oktober 2020

Welt.de Nachrichten

**Datenschutzerklärung WELT DIGITAL**

Veröffentlicht am 24.08.2020 | Lesedauer: 42 Minuten

WELT nimmt Datenschutz ernst und ist stets bemüht, alle personenbezogenen Daten in Übereinstimmung mit dem jeweils geltenden Datenschutzrecht zu erheben und zu nutzen.

[0](https://www.welt.de/services/article157550705/Datenschutzerklaerung-WELT-DIGITAL.html#Comments)

Wir freuen uns sehr über Ihr Interesse an WELT Digital. Mit dieser Datenschutzerklärung informieren wir Sie über Art, Umfang und Zweck der von uns verarbeiteten personenbezogenen Daten und Ihre Rechte als betroffene Person.

**1. Verantwortlicher**

Verantwortlich für die Datenverarbeitung gemäß Art.4 Nr. 7 DSGVO ist vorbehaltlich abweichender Angaben in dieser Datenschutzerklärung die Axel Springer SE, Axel-Springer-Str. 65, 10888 Berlin, Telefon: +49 30 2591 0 (nachfolgend auch „wir“ oder „uns“).

Verantwortlich für die Verarbeitung personenbezogener Daten für Bilanz Deutschland – das deutsche Wirtschaftsmagazin (Print und Digital), ist die Bilanz Deutschland Wirtschaftsmagazin GmbH.

Wir gestalten Internetseiten aus unserer Website auch als Accelerated Mobile Pages (AMP). Rufen Sie, zB nach einer Google-Suche mit Ihrem Smartphone, eine dieser Internetseiten auf, wird diese AMP möglicherweise nicht von unseren Servern, sondern direkt aus dem Zwischenspeicher (Cache) von Drittanbietern wie z.B. Google ausgeliefert. In diesen Fällen erscheint in der Adresszeile Ihres Browsers auf der Ebene der Second Level Domain nicht unser Domainname (unsere Internetadresse), sondern z.B. der Domainname von Google bzw. „ampproject.org“ Bei solchen Aufrufen aus dem Zwischenspeicher von Google oder sonstigen Drittanbietern haben wir keinen Einfluss auf die Datenverarbeitung durch diese. Wir achten darauf, dass wir über unsere AMP keine personenbezogenen Daten erheben und haben deshalb in der AMP-Version alle Kontaktformulare deaktiviert.

In unsere Website sind Serviceseiten von Partnern integriert („Partnerserviceseite“). Sie erkennen diese an der entsprechenden Kennzeichnung (z.B. „Ein Service von“). Die Partnerserviceseite wird von dem dort angegebenen Partner bereitgestellt. Verantwortlich für den Inhalt der Partnerserviceseite und die dort stattfindenden Datenverarbeitungsvorgänge gemäß Art. 4 Nr. 7 DSGVO ist – mit Ausnahme des Header und Footer der Website – der Partner. Informationen zum Partner erhalten Sie in dem in der Partnerserviceseite verlinkten Impressum des Partners. Informationen zu den über die Partnerserviceseite stattfindenden Datenverarbeitungsvorgängen und Ihren Rechten als betroffene Person entnehmen Sie bitte der ebenfalls dort verlinkten Datenschutzerklärung des Partners.

**2. Aufruf der Website**

Wenn Sie unser Angebot nutzen, werden durch uns automatisch verschiedene Daten erfasst und verarbeitet, wie z.B.:

- Informationen über das zugreifende Endgerät und die verwendete Software

- Datum und Uhrzeit des Zugriffs

- Cookies (Sonderkategorien)

- Websites, von denen der Nutzer auf unsere Website gelangt oder die der Nutzer über unsere Website aufruft

- IP-Adresse

Die zumindest vorübergehende Speicherung der IP-Adresse ist technisch erforderlich, um eine Auslieferung der Website an. den Rechner des Nutzers zu ermöglichen. Unsere Server speichern Ihre IP-Adresse außerdem für bis zu 14 Tage zu eigenen Sicherheitszwecken (Art. 6 Abs. 1 lit. f DSGVO).

**3. Registrierung**

Für das Bereitstellen bestimmter Inhalte oder Leistungen auf unseren Websites ist eine Anmeldung mittels eines bestehenden Benutzerkontos erforderlich. Für das Benutzerkonto ist eine entsprechende Registrierung notwendig. Wir setzen dabei unseren portalübergreifenden Dienst myPass ein, der Ihnen die Anmeldung auf allen Websites der Axel Springer SE ermöglicht, die myPass ebenfalls integriert haben. Für die Nutzung von myPass gelten die [Nutzungsbedingungen von mypass](https://www.mypass.de/information/nutzungsbedingungen-fuer-mypass). Mehr Informationen zu myPass finden Sie hier: [www.mypass.de](http://www.mypass.de/) Weitere Informationen zur Datenverarbeitung können Sie dem [Datenschutzhinweis](https://www.mypass.de/datenschutz)für den Single-Sign-On-Dienst myPass entnehmen. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b DSGVO.

**4. Abonnement und zahlungspflichtige Dienste**

Beim Abschluss eines Abonnements oder bei Bezug eines zahlungspflichtigen Dienstes nutzen wir Ihre Vertragsstammdaten einschließlich Kontaktdaten zur Vertragsdurchführung und -erfüllung, wie dies beispielsweise bei Verarbeitungsvorgängen der Fall ist, die für eine Lieferung von Waren oder die Erbringung einer sonstigen Leistung oder Gegenleistung, sowie die Durchsetzung von Rechtsansprüchen oder Forderungen notwendig ist (Art. 6 Abs. 1 lit. b DSGVO). Gleiches gilt für solche Verarbeitungsvorgänge die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind, etwa in Fällen von Anfragen zu unseren Produkten oder Leistungen. Im Falle von bezahlpflichtigen Diensten verarbeiten wir gewisse Daten, weil wir einer rechtlichen Verpflichtung unterliegen, durch welche eine Verarbeitung von personenbezogenen Daten erforderlich wird, wie beispielsweise zur Erfüllung steuerlicher Pflichten (Art. 6 Abs. 1 lit. c DSGVO i.V.m. § 147 AO; Aufbewahrungspflicht 10 Jahre). Dazu gehört aus umsatzsteuerrechtlichen Gründen auch die Speicherung der IP-Adresse des Geräts, von dem aus Sie bei Abschluss des Vertrages auf die betreffende Website zugegriffen haben, in unseren Unternehmens-Informationssystemen.

Für den Fall, dass Sie einen zahlungspflichtigen Dienst nutzen oder etwas über unsere Website erwerben, bieten wir verschiedene Zahlungsmethoden folgender Drittanbieter an, die jeweils verantwortlich für die Datenverarbeitung gemäß Art. 4 Nr. 7 DSGVO sind:

Zudem verarbeiten wir Ihre ungekürzte IP-Adresse bzw. Ihre pseudonyme ID während der Nutzung unseres Angebots, zu dem Zweck und in unserem Interesse, die Leistungsfähigkeit und Performance unseres Angebots zu messen. Nutzungsprofile werden dabei nicht erstellt. Ihre IP-Adresse bzw. pseudonyme ID wird unmittelbar nach Schließung der jeweiligen Sitzung automatisiert anonymisiert. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. f DSGVO.

**Saferpay**

Wir haben auf dieser Website den Zahlungsdienstleister Saferpay integriert. Betreibergesellschaft ist SIX Payment Services AG, Hardturmstrasse 201, 8005 Zürich. Wählt ein Nutzer diese Zahlart, wird er direkt zu dem Dienstleister weitergeleitet, sodass dieser ab dem Zeitpunkt für die Verarbeitung verantwortlich ist. Wir übermitteln an Saferpay die folgenden Daten: zu bezahlender Betrag und Referenznummer. Weitere Informationen finden Sie unter <https://www.six-payment-services.com/de/services/legal/privacy-statement.html>.

**Lastschrift Komplett und monatliche Zahlungsweise**

Wir haben auf dieser Website die Zahlungsmethoden „Lastschrift Komplett“ und „Monatliche Zahlungsweise“ der Arvato Payment Solutions GmbH, Gütersloher Str. 123, 33415 Verl („Arvato“) integriert. Diese Zahlungsmethoden können nur gewährt werden, wenn Sie Arvato eine Ermächtigung zur Einziehung der Forderung und Ihre Einwilligung in eine vorherige Bonitätsprüfung und Missbrauchserkennung durch Arvato erteilt haben. Nach erfolgreicher Bonitätsprüfung treten wir die während der vereinbarten Mindestvertragslaufzeit fälligen Forderungen an Arvato ab, die in diesem Zeitraum dann auch die Einziehung der monatlichen Teilbeträge übernimmt. Zu den vorgenannten Zwecken übermitteln wir an Arvato Ihren Namen, Ihr Geburtsdatum, Ihre Anschrift, Ihre E-Mail-Adresse, Ihre Bankverbindungsdaten, die IP-Adresse, sowie Informationen über die Forderungshöhe und die Fälligkeit der Teilforderungen und Angaben zu den von Ihnen bestellten Artikeln (z.B. Bestellwert, Produktgruppe, Warenwert, ggf. Anfragekanal und Lieferart). Rechtsgrundlage für die Datenübermittlung ist Art. 6 Abs. 1 lit. b und Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse besteht darin, Ihnen auch risikobehaftete Zahlarten, wie Monatliche Zahlungsweise oder Lastschrift Komplett, anbieten zu können. Das berechtigte Interesse von Arvato besteht darin, vor Gewährung der Zahlarten, die alle ein kreditorisches Risiko mit sich bringen, möglichst gut einschätzen zu können, ob Sie den eingegangenen Zahlungsverpflichtungen nachkommen werden. Verantwortlich für die weitere Datenverarbeitung gemäß Art. 4 Nr. 7 DSGVO ist ausschließlich Arvato. Detaillierte datenschutzrechtliche Informationen zu Arvato finden Sie unter folgendem Link <https://documents.myafterpay.com/tnp/privacy-statement/de_de/>

**Amazon Payment**  
Amazon Pay ist eine Zahlungsmöglichkeit von Amazon Europe Core S.à r.l. (Société à responsabilité limitée), 5 Rue Plaetis, L-2338 Luxemburg. Mit Amazon Pay können Sie somit auf Websites von Drittanbietern sicher einkaufen, ohne Ihre Zahlungsdaten offenlegen zu müssen. Des Weiteren entstehen Ihnen keine zusätzlichen Kosten, wenn Sie mit Amazon Pay bezahlen. Wenn Sie bereits ein Amazon.de-Kundenkonto haben, wurde automatisch ein Amazon Pay-Konto für Sie erstellt. Dieses wird aktiviert, wenn Sie erstmals auf der Website eines Drittanbieters, der Amazon Pay akzeptiert, bestellen. Dieses Konto ist mit Ihrem Amazon.de-Kundenkonto verknüpft und Sie können sofort mit der dort hinterlegten Zahlungsart - entweder per Bankeinzug oder mit Kreditkarte - bezahlen. Amazon Pay gibt die in Ihrem Amazon.de-Kundenkonto hinterlegten Zahlungsdaten nicht an den Verkäufer weiter und auch Sie müssen diese bei Bestellaufgabe nicht angeben. [Hier](https://pay.amazon.com/de/help/201754560) erfahren Sie mehr zur Zahlung mit Amazon Pay auf Websites von Drittanbietern. Weitere Informationen finden Sie auf der Amazon Pay-Website unter <https://pay.amazon.com/de>.

**PayPal**

Wir haben auf dieser Website die Zahlungsmöglichkeit PayPal integriert. PayPal ist ein Online-Zahlungsdienstleister der PayPal (Europe) S.à.r.l. & Cie. S.C.A., 22-24 Boulevard Royal, 2449 Luxembourg, Luxemburg. Zahlungen werden über sogenannte PayPal-Konten abgewickelt, die virtuelle Privat- oder Geschäftskonten darstellen. Zudem besteht bei PayPal die Möglichkeit, virtuelle Zahlungen über Kreditkarten abzuwickeln, wenn ein Nutzer kein PayPal-Konto unterhält. Ein PayPal-Konto wird über eine E-Mail-Adresse geführt, weshalb es keine klassische Kontonummer gibt. PayPal ermöglicht es, Online-Zahlungen an Dritte auszulösen oder auch Zahlungen zu empfangen. PayPal übernimmt ferner Treuhänderfunktionen und bietet Käuferschutzdienste an. Wählt die betroffene Person während des Bestellvorgangs in unserem Online-Shop als Zahlungsmöglichkeit „PayPal“ aus, werden automatisiert Daten der betroffenen Person an PayPal übermittelt. Mit der Auswahl dieser Zahlungsoption willigt die betroffene Person in die zur Zahlungsabwicklung erforderliche Übermittlung personenbezogener Daten ein. Bei den an PayPal übermittelten personenbezogenen Daten handelt es sich in der Regel um Vorname, Nachname, Adresse, Email-Adresse, IP-Adresse, Telefonnummer, Mobiltelefonnummer oder andere Daten, die zur Zahlungsabwicklung notwendig sind. Zur Abwicklung des Kaufvertrages notwendig sind auch solche personenbezogenen Daten, die im Zusammenhang mit der jeweiligen Bestellung stehen. Die Übermittlung der Daten bezweckt die Zahlungsabwicklung und die Betrugsprävention. Wir werden PayPal personenbezogene Daten insbesondere dann übermitteln, wenn ein berechtigtes Interesse für die Übermittlung gegeben ist.

Die zwischen PayPal und dem für uns ausgetauschten personenbezogenen Daten werden von PayPal unter Umständen an Wirtschaftsauskunfteien übermittelt. Diese Übermittlung bezweckt die Identitäts- und Bonitätsprüfung. PayPal gibt die personenbezogenen Daten gegebenenfalls an verbundene Unternehmen und Leistungserbringer oder Subunternehmer weiter, soweit dies zur Erfüllung der vertraglichen Verpflichtungen erforderlich ist oder die Daten im Auftrag verarbeitet werden sollen.

Die betroffene Person hat die Möglichkeit, die Einwilligung zum Umgang mit personenbezogenen Daten jederzeit gegenüber PayPal zu widerrufen. Ein Widerruf wirkt sich nicht auf personenbezogene Daten aus, die zwingend zur (vertragsgemäßen) Zahlungsabwicklung verarbeitet, genutzt oder übermittelt werden müssen.

Die geltenden Datenschutzbestimmungen von PayPal können unter <https://www.paypal.com/de/webapps/mpp/ua/privacy-full> abgerufen werden.

**Stripe**

Wenn Du Dich für eine Zahlungsart des Paymentdienstleisters Stripe entscheidest, erfolgt die Zahlungsabwicklung über den Paymentdienstleister Stripe Payments Europe Ltd, Block 4, Harcourt Centre, Harcourt Road, Dublin 2, Ireland, an den wir Deine im Rahmen des Bestellvorgangs mitgeteilten Informationen nebst den Informationen über Deine Bestellung (Name, Anschrift, Kontonummer, Bankleitzahl, evtl. Kreditkartennummer, Rechnungsbetrag, Währung und Transaktionsnummer) weitergeben. Die Weitergabe Deiner Daten erfolgt ausschließlich zum Zwecke der Zahlungsabwicklung mit dem Payment-Dienstleister Stripe Payments Europe Ltd. Nähere Informationen zum Datenschutz von Stripe findest Du unter: <https://stripe.com/de/terms>.

**5. Mein WELT-Konto**

Sofern Sie sich für Mein WELT-Konto registriert haben, führen wir Ihre Nutzer-ID mit Ihrer im Registrierungsprozess angegebenen E-Mail-Adresse und mit pseudonymisierten Daten Ihres Nutzerverhaltens bei WELT (Nutzungsdaten) sowie, soweit Sie über unsere Website ein kostenpflichtiges Produkt bestellt haben – mit Ihren Bestelldaten (d.h. das/die von Ihnen bestellten Produkt/-e, das Datum der Bestellung und das Datum des möglichen Endes Ihre Abonnements) zusammen, um Ihnen die personalisierten Dienste bei WELT erbringen zu können.

Bei Ihrer Nutzer-ID handelt es sich um eine Ihnen bei der Registrierung nach dem Zufallsprinzip generierten Identifikationsnummer, unter der Sie als Nutzer geführt werden und die uns ermöglicht, Sie in der Folge als berechtigen Nutzer identifizieren und Ihnen Zugang zu den Diensten geben zu können.

Die betreffenden Nutzungsdaten erheben wir durch Cookies und ähnliche Technologien. Bei den erfassten Nutzungsdaten handelt es ich u.a. um die folgenden Informationen:

* Häufigkeit und Dauer der Nutzung
* Artikel- und Bildaufrufe
* Abspielen von Audio- und Videoformaten
* Region der Nutzung
* Aktionen (z.B. Inhalte teilen, Kommentare)

Wir verarbeiten die Daten zu dem Zweck, Ihnen bei WELT auf Ihre Interessen und Ihre Nutzung abgestimmte Inhalte anzeigen zu können und Ihnen per E-Mail für Sie interessante Artikel und Inhalte zu empfehlen. Sofern Sie die Zusendung personalisierter Artikelempfehlungen per E-Mail nicht wünschen sollten, haben Sie jederzeit die Möglichkeit, diesen Dienst zu deaktivieren, z.B. durch Anklicken des hierfür vorgesehenen Links in jeder Artikelempfehlung bzw. im Bereich „Meine Newsletter“.

Rechtsgrundlage der Datenverarbeitung ist zum einen die Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) und zum anderen unser Interesse, Ihr Nutzungserlebnis aufgrund der Berücksichtigung Ihrer Interessen zu optimieren (Art. 6 Abs. 1 lit. f DSGVO).

**6. Mailings und Newsletter**

Ihre im Zuge der Registrierung oder im Rahmen der Vertragsdurchführung erhobene E-Mail-Adresse verwenden wir außerdem, um Sie per E-Mail über eigene ähnliche Waren oder Dienstleistungen sowie über bestehende Abonnements oder generell über unsere Onlinedienste zu informieren, sofern wir Sie bei Erhebung der E-Mail-Adresse hierauf hingewiesen und Sie dem nicht widersprochen haben. Die Verarbeitung der E-Mail-Adresse erfolgt in diesem Fall auf Grundlage unseres berechtigten Interesses an der Bewerbung unserer Waren und Dienstleistungen (Art. 6 Abs. 1 lit. f DSGVO, § 7 Abs. 3 UWG). Sie haben jederzeit die Möglichkeit, der Zusendung dieser Informationen über weitere Produktangebote zu widersprechen, z.B. durch Anklicken des hierfür in jeder dieser E-Mails vorgesehenen Abbestelllinks.

Sofern Sie einen unserer Mailings bzw. Newsletter bestellt haben, nutzen wir Ihre E-Mail-Adresse darüber hinaus, um Ihnen den von Ihnen bestellten Newsletter zuzusenden. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b DSGVO bzw. Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung mit Wirkung für die Zukunft zu widerrufen bzw. den bestellten Newsletter wieder abzubestellen, z.B. durch Anklicken des hierfür in jedem Newsletter vorgesehenen Abbestelllinks.

**7. Personalisierte Produkt- und Medienangebote per E-Mail bzw. Push-Nachrichten**

Sofern Sie Ihre Einwilligung in die Zusendung von Newslettern per E-Mail und/oder Push-Nachrichten mit Produktangeboten und/oder Medienangebote auf Basis Ihrer persönlichen Nutzung der Axel Springer Medien erteilt haben, führen wir Ihr pseudonymes Nutzungsprofil (Nutzungsdaten) mit Ihrer nach dem Zufallsprinzip generierten Identifikationsnummer (Nutzer-ID) und Ihrer E-Mail-Adresse zusammen. Bei den erfassten Nutzungsdaten handelt es ich u.a. um die folgenden Informationen:

- Häufigkeit und Dauer der Nutzung

- Artikel- und Bildaufrufe

- Abspielen von Audio- und Videoformaten

- Region der Nutzung

- Aktionen (z.B. Inhalte teilen, Kommentare)

Die betreffenden Nutzungsdaten erheben wir mittels Cookies und ähnlichen Technologien gemäß den Ausführungen in dieser Datenschutzerklärung. Diese Datenzusammenführung erfolgt zu dem Zweck, Ihnen per E-Mail entsprechend Ihren Interessen auf Basis Ihres Nutzungsverhaltens interessante Werbung gemäß Ihrer Einwilligung zuzusenden.

Soweit Sie über unsere Website ein kostenpflichtiges Produkt bestellt haben, führen wir mit Ihrer Einwilligung darüber hinaus Daten über Ihre Bestellung(en), wie das von Ihnen bestellte Produkt, das Datum der Bestellung und das Datum des möglichen Endes Ihre Abonnements zu den vorstehend genannten Daten hinzu. Dies erfolgt zu dem Zweck, Ihnen auch unter Berücksichtigung der von Ihnen erworbenen Produkte für Sie interessante Werbung auszuspielen. Rechtsgrundlage für die Zusammenführung der Daten zu diesem Zweck ist Art. 6 Abs. 1 lit a DSGVO. Sie können Ihre diesbezügliche Einwilligung jederzeit mit Wirkung für die Zukunft insgesamt widerrufen, z.B. durch Anklicken des hierfür in jedem personalisierten Newsletter vorgesehenen Abbestelllinks.

**8. E-Mail-Tracking**

Sofern Sie einen unserer Mailings oder Newsletter bzw. personalisierte Produkt- und Medienangebote per E-Mail abonniert haben, sind in den E-Mails sind sogenannte Zählpixel integriert, zu dem Zweck und in unserem Interesse, unseren Newsletter optimieren zu können. Wir erhalten hierdurch die Information, welcher Browser und welches Betriebssystem verwendet wird, welche IP-Adresse gerade zugreift und zugleich, wer der Provider ist. Zudem wird erkannt, ob die E-Mail gelesen und ob anschließend der in der E-Mail integrierte Link angeklickt und die jeweilige Website über diese IP-Adresse besucht wurde. Zusätzlich wird die Anzahl der Zugriffe auf die Webseite gezählt sowie die entsprechende Tageszeit festgehalten, wann die E-Mail abgerufen und der Zugriff getätigt wurde. Auch der ungefähre Standort des Nutzers wird übermittelt. Sollten Sie dies nicht wünschen, können Sie den Newsletter jederzeit wie vorstehend beschrieben abbestellen und damit Ihre Einwilligung widerrufen. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO.

**9. Geo-Lokalisierung**

Auf der Grundlage der gekürzten IP-Adresse können wir auf allen unseren Websites, die aus einer bestimmten Region abgerufen werden, Inhalte mit regionalem Bezug anzeigen. Diese sogenannte Geo-Lokalisierung, also die Zuordnung eines Websiteaufrufs zum Ort des Aufrufs, erfolgt grundsätzlich ausschließlich auf der Grundlage der anonymisierten IP-Adresse und nur bis zur geographischen Ebene der Bundesländer / Regionen. Aus den so gewonnenen geographischen Informationen kann kein Rückschluss auf den konkreten Aufenthaltsort eines Nutzers gezogen werden.

**10. Kommentarfunktion und Umfragen**

Wir bieten auf unserer Website und in Blogs sowie auf allgemeinen Feedback-Seiten vereinzelt die Möglichkeit an, Kommentare und Feedback abzugeben oder Bugs und fehlerhafte Inhalte zu melden sowie an Umfragen teilzunehmen, wobei zusätzliche personenbezogene Daten gespeichert werden, die Sie von sich aus angeben. Wir verarbeiten in diesen Fällen die Daten, die Sie uns übermitteln. Wenn Ihre Eingaben zur Veröffentlichung bestimmt sind und Sie hierzu eine Einwilligung abgegeben haben, können Sie auf unseren Online Diensten Kommentare abgeben und abonnieren. Das gleiche gilt bei Umfragen, an denen Sie teilnehmen. Wenn Sie einen Kommentar veröffentlichen möchten, müssen Sie die hierfür vorgesehenen Felder ausfüllen. Sie können hierbei auch ein Pseudonym verwenden. Wenn Sie die Felder nicht ausfüllen, können Sie keinen Kommentar veröffentlichen. Wir erheben und verarbeiten die von Ihnen angegebenen Daten, um Ihren Kommentar wunschgemäß veröffentlichen und auf mögliche Verstöße gegen unsere Netiquette-Regeln überprüfen zu können (Art. 6 Abs. 1 lit. b DSGVO). Insbesondere benötigen wir hierbei auch Ihre E-Mail-Adresse, um Sie im Falle von Beanstandungen Ihres Kommentars oder Ihrer Meldung kontaktieren und Ihnen die Möglichkeit zur Stellungnahme geben zu können (Art. 6 Abs. 1 lit. c DSGVO).

Zur Analyse von Nutzerkommentaren hinsichtlich der Einhaltung unserer Netiquette-Regeln nutzen wir das Moderations-Tool Conversario der ferret go GmbH, Brauerstraße 14, 16321 Bernau bei Berlin (ferret go). Folgende Daten werden in unserem Auftrag (Art. 28 DSGVO) erfasst und gespeichert: Conversario Facebook: NutzerID / NutzerName (Facebook Name) / Nutzerbild / Kommentartext / KommentarID / Datum & Uhrzeit des Kommentars. Conversario Onsite: NutzerName (nicht Personen identifizierbar) Kommentartext / KommentarID / Datum & Uhrzeit des Kommentars.

**11. Ihre Kontaktaufnahme**

Bei Ihrer Kontaktaufnahme mit uns über eines unserer Kontaktformulare oder per E-Mail werden die von Ihnen mitgeteilten Daten (Ihre E-Mail-Adresse, ggf. Ihr Name und Ihre Telefonnummer) von uns verarbeitet, um Ihre Anfrage zu bearbeiten. Die in diesem Zusammenhang anfallenden Daten löschen wir, wenn sie für den vorgenannten Zweck nicht mehr erforderlich sind, sofern der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 Satz 1 lit. f DSGVO. Wenn Sie uns personenbezogene Daten einer anderen Person mitteilen, müssen Sie dazu die ausdrückliche vorherige Einwilligung dieser Person einholen und sie darüber informieren, wie wir personenbezogene Daten gemäß unserer Datenschutzerklärung verarbeiten.

Vereinzelt stellen wir auch Kontaktformulare von Drittanbietern bereit, zu dem Zweck und in dem Interesse, Ihnen eine unmittelbare Kontaktaufnahme zu dem jeweils in dem Kontaktformular ausgewiesenen Drittanbieter zu ermöglichen. Die von Ihnen in das Kontaktformular eingegebenen personenbezogenen Daten werden über eine Schnittstelle direkt an den Drittanbieter weitergeleitet. Wir haben keinen Zugriff auf die Daten, eine (Zwischen-)Speicherung der Daten findet nicht statt. Informationen zur Datenverarbeitung entnehmen Sie der jeweils im Kontaktformular verlinkten Datenschutzerklärung des Drittanbieters. Rechtsgrundlage für die Datenübermittlung ist Art. 6 Abs. 1 lit. b bzw. Art. 6 Abs. 1 lit. f DSGVO.

**12. Gewinnspiele**

Sofern Sie an einem Gewinnspiel teilnehmen, können Sie die weiteren Informationen zur über die im Rahmen der Gewinnspielteilnahme stattfindende Datenverarbeitung dem Datenschutzhinweis des jeweiligen Gewinnspiels entnehmen.

**13. Ort der Verarbeitung**

Wir verarbeiten Daten auch in Staaten außerhalb des Europäischen Wirtschaftsraumes („EWR“). Um den Schutz Ihrer Persönlichkeitsrechte auch im Rahmen dieser Datenübertragungen zu gewährleisten, bedienen wir uns bei der Ausgestaltung der Verhältnissemit den eingesetzten Diensten in Drittländern der Standardvertragsklauseln der EU-Kommission gemäß Art. 46 Abs. 2 lit. c DSGVO.

[Standardvertragsklauseln mit Auftragsverarbeitern](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32010D0087&from=DE)

[Standardvertragsklauseln mit Verantwortlichen](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32004D0915&from=DE).

**14. Weitergabe Ihrer Daten an Dritte**

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, wenn die Übermittlung erforderlich ist, um unsere vertraglichen Verpflichtungen Ihnen gegenüber zu erfüllen und dies ersichtlich bei oder gemeinsam mit einem anderen Anbieter erfolgt (z. B. bei Kooperationen), wir zur Weitergabe in sonstiger Weise berechtigt oder verpflichtet sind, oder Sie uns eine entsprechende Einwilligung erteilt haben.

Zur Erbringung unserer Leistung können ausgewählte personenbezogene Daten innerhalb unseres Unternehmens an bestimmte Abteilungen mitgeteilt werden. Dazu gehören Mitarbeiter der Abteilungen Buchhaltung, Product Management, Marketing und IT.

Sofern Sie ein Abo mit uns haben, erfolgt die Logistik, insbesondere der Versand bzw. die Zustellung durch verschiedene Zustellpartner.

In bestimmten Fällen setzen wir auch externe Dienstleister oder verbundene Unternehmen ein, die von uns beauftragt sind, Daten für uns weisungsgebunden zu verarbeiten. Solche Dienstleister werden von uns gemäß Art. 28 DSGVO vertraglich als Auftragsverarbeiter verpflichtet und dürfen Ihre Daten zu keinen anderen Zwecken weiterverwenden. Von uns eingesetzte Auftragsverarbeiter erbringen für uns insbesondere die folgenden Dienstleistungen: Abonnementverwaltung, Anmeldedienst(e), Bezahldienst(e), Content Recommendation, Hosting, Inkasso / Forderungsmanagement, Kundenservice, Logistik und Versand, Newsletterversand, Prämienversand, Umfrage-/Kommentardienst(e), Vertrieb, Wartung und Support und Webanalyse.

**15. Cookies und ähnliche Technologien**

Um unser Angebot anbieten zu können und die Sicherheit der Website zu gewährleisten, Betrug zu verhindern und Fehler zu beheben sowie Inhalte auf der Website technisch bereitzustellen, ist der Einsatz bestimmter Cookies und ähnlicher Technologien erforderlich (Sonderkategorien). Ferner werden die von Ihnen in der Privatsphäre vorgenommenen Einstellungen bzw. erteilten Einwilligungen und Widersprüche in Cookies auf Ihrem Endgerät gespeichert. Der Einsatz dieser Cookies ist erforderlich, damit wir den von Ihnen angefragten Dienst erbringen können. Weitere Informationen zu diesen Sonderkategorien von Cookies können Sie der Privatsphäre entnehmen.

Um den Umfang der Nutzung unserer kostenpflichtigen Bereiche zu messen, werden Informationen in einem besonderen Messmodul zusammen mit einer speziell für die Messung der Seiten- bzw. Inhalteabrufe generierten Zufallsnummer („M-ID“) hinterlegt. Bei der Nutzung über einen Browser wird zugleich ein Cookie gesetzt, sofern Ihre Geräteeinstellungen dies zulassen. Im Cookie wird die M-ID gespeichert, um die Anzahl der Aufrufe unserer Inhalte zu ermitteln. Diese Datenerhebung und -speicherung ist notwendig, damit festgestellt werden kann, wie oft Inhalte auf Ihrem Gerät kostenlos genutzt wurden.

Soweit nicht anders bestimmt, setzen wir weitere Cookies und ähnliche Technologien auf dieser Website nur vorbehaltlich Ihrer Einwilligung. Diese verwenden wir und unsere Partner, um Daten auf Ihrem Endgerät zu speichern und zu verarbeiten, u. a. zu dem Zweck, Anzeigen und Inhalte basierend auf einem Nutzungsprofil zu personalisieren, dem Profil Daten hinzuzufügen, um Anzeigen und Inhalte besser zu personalisieren, die Leistung von Anzeigen und Inhalten zu messen, Erkenntnisse über die Zielgruppen, die die Anzeigen und Inhalte gesehen haben, abzuleiten, die Benutzerfreundlichkeit, Systeme und Software aufzubauen oder zu verbessern. Ohne die Erteilung einer Einwilligung für das Setzen von Cookies sind unter Umständen nicht alle Funktionen unserer Website vollumfänglich nutzbar.

Cookies sind kleine Dateien, die Ihr Browser auf Ihrem Gerät in einem dafür vorgesehenen Verzeichnis ablegt. Durch sie kann u. a. festgestellt werden, ob Sie eine Website schon einmal besucht haben. Viele Cookies enthalten eine sogenannte Cookie-ID. Eine Cookie-ID ist eine eindeutige Kennung des Cookies. Sie besteht aus einer Zeichenfolge, durch welche Websites und Server dem konkreten Internetbrowser zugeordnet werden können, in dem das Cookie gespeichert wurde. Dies ermöglicht es den besuchten Websites und Servern, den individuellen Browser von anderen Internetbrowsern, die andere Cookies enthalten, zu unterscheiden. Ein bestimmter Internetbrowser kann über die eindeutige Cookie-ID wiedererkannt und identifiziert werden. Cookies können ohne zusätzliche Informationen Sie als Person nicht identifizieren.

Weitere Informationen zu den eingesetzten Cookies finden Sie an entsprechender Stelle in den Einstellungen Ihrer Privatsphäre. Dort haben Sie auch jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung mit Wirkung für die Zukunft zu widerrufen. Bereits gesetzte Cookies können von Ihnen darüber hinaus jederzeit über einen Internetbrowser oder andere Softwareprogramme gelöscht werden. Dies ist in allen gängigen Internetbrowsern möglich. Bitte beachten Sie, dass in diesem Fall auch die von Ihnen vorgenommenen Einstellungen in der Privatsphäre gelöscht werden und bei einem erneuten Besuch unserer Website erneut vorgenommen werden müssten. Die Laufzeit der eingesetzten Cookies ist vorbehaltlich abweichender Angaben auf die Dauer von maximal einem Jahr beschränkt.

**16. Auswahl einfacher Anzeigen**

Zu dem Zweck und in dem Interesse, die Auswahl und Ausspielung der zur Refinanzierung unseres Angebots ausgespielten Anzeigen zu optimieren, die Häufigkeit und Reihenfolge der Anzeige-Einblendungen zu steuern und um zu verhindern, dass eine Anzeige in einem ungeeigneten redaktionellen Umfeld (brand-unsafe) eingeblendet wird, verarbeiten wir Echtzeit-Informationen über den Kontext, in dem die Anzeige dargestellt wird, einschließlich Informationen über das inhaltliche Umfeld sowie das verwendete Gerät, wie z. B. Gerätetyp und -funktionen, Browser-Kennung, URL, IP-Adresse und die ungefähren Standortdaten eines Nutzers. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. f DSGVO. Sie haben jederzeit die Möglichkeit, die Auswahl einfacher Anzeigen in den Einstellungen der Privatsphäre abzulehnen und damit der Datenverarbeitung zu diesem Zweck zu widersprechen. . Für die vorgenannten Zwecke bedienen wir uns auch der Dienste nachfolgend aufgeführter Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch diese Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen der Drittanbieter entnehmen:

* + - **AdDefend** (AdDefend GmbH, Borselstrasse 3, 22765 Hamburg), <https://www.addefend.com/de/datenschutzerklarung/>
    - **AWIN (**AWIN AG, Stralauer Allee 2, 10245 Berlin, Deutschland), https://www.awin.com/de/rechtliches/privacy-policy
    - **Bing Ads** (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), https://privacy.microsoft.com/de-de/privacystatement
    - **Google Ads** (ehem. AdWords) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Google AdSense** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Google Dynamic Remarketing** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Google Floodlight** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Google Marketing Plattform** (ehem. DoubleClick) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy](http://www.google.de/intl/de/policies/privacy)
    - **Taboola** (Taboola Inc. (28 West 23 St. 5 fl., New York, NY 10010, USA), <https://www.taboola.com/privacy-policy>
    - **Xandr** (ehemals AppNexus)-(Xandr Inc., 28 W. 23rd Street, New York, New York, 10010, USA ) https://www.xandr.com/privacy/platform-privacy-policy/#choicesContact Impact GmbH

**17. Personalisiertes Anzeigenprofil**

Vorbehaltlich Ihrer Einwilligung setzen wir Dienste ein zu dem Zweck, die zur Refinanzierung unseres Angebots ausgespielten Anzeigen an Ihren Interessen auf Basis Ihres Nutzungsverhaltens auszurichten. Zu diesem Zweck wird ein Profil Ihrer Nutzung mit Informationen zu Ihren Aktivitäten, Interessen, den Besuchen auf Webseiten oder der Verwendung von Anwendungen, demographischen Informationen oder des Standorts erstellt. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Für die vorgenannten Zwecke bedienen wir uns auch der Dienste nachfolgend aufgeführter Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch diese Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen der Drittanbieter entnehmen:

* + - **AdDefend** (AdDefend GmbH, Borselstrasse 3, 22765 Hamburg), <https://www.addefend.com/de/datenschutzerklarung/>
    - **AWIN (**AWIN AG, Stralauer Allee 2, 10245 Berlin, Deutschland), https://www.awin.com/de/rechtliches/privacy-policy
    - **Bing Ads** (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), https://privacy.microsoft.com/de-de/privacystatement
    - **Google Ads** (ehem. AdWords) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Google AdSense** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Google Dynamic Remarketing** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Google Floodlight** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Google Marketing Plattform** (ehem. DoubleClick) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy](http://www.google.de/intl/de/policies/privacy)
    - **Google MobileAds SDK**(Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Taboola** (Taboola Inc. (28 West 23 St. 5 fl., New York, NY 10010, USA), https://www.taboola.com/privacy-policy

**18. Auswahl personalisierter Anzeigen**

Vorbehaltlich Ihrer Einwilligung setzen wir Dienste ein zu dem Zweck, Ihnen für Sie interessante Anzeigen auf Basis eines von Ihnen vorbehaltlich Ihrer Einwilligung erstellten personalisierten Anzeigenprofils ausspielen zu können. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Hierbei bedienen wir uns auch der Dienste nachfolgend aufgeführter Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch die eingesetzten Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* **AdDefend** (AdDefend GmbH, Borselstrasse 3, 22765 Hamburg), <https://www.addefend.com/de/datenschutzerklarung/>
* **AWIN (**AWIN AG, Stralauer Allee 2, 10245 Berlin, Deutschland), https://www.awin.com/de/rechtliches/privacy-policy
* **Bing Ads** (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), https://privacy.microsoft.com/de-de/privacystatement
* **Google Ads** (ehem. AdWords) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
* **Google AdSense** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
* **Google Dynamic Remarketing** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
* **Google Floodlight** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
* **Google Marketing Plattform** (ehem. DoubleClick) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy](http://www.google.de/intl/de/policies/privacy)
* **Taboola** (Taboola Inc. (28 West 23 St. 5 fl., New York, NY 10010, USA), https://www.taboola.com/privacy-policy

**19. Personalisiertes Inhalts-Profil**

Zu dem Zweck und in unserem Interesse, die Auswahl von Inhalten in unserem Angebot auf Ihr Nutzungsverhalten und demzufolge an Ihren mutmaßlichen Interessen auszurichten erstellen wir ein Profil Ihrer Nutzung mit Informationen zu den Aktivitäten, Interessen und Besuchen auf Webseiten oder der Verwendung von Anwendungen, demographischen Informationen oder des Standorts. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. f DSGVO. Sie haben jederzeit die Möglichkeit, die Erstellung von personalisierten Inhalts-Profilen in den Einstellungen der Privatsphäre abzulehnen und damit der Datenverarbeitung zu diesem Zweck zu widersprechen.

Vorbehaltlich Ihrer Einwilligung bedienen wir uns dabei auch der Dienste der nachfolgend aufgeführten Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Rechtsgrundlage der Datenverarbeitung ist in diesen Fällen Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Weitere Informationen zur Datenverarbeitung durch die Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* **Instagram** (Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland) <https://www.instagram.com/legal/privacy/>
* **LinkedIn** (LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Irland) <https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy>
* **SoundCloud**(SoundCloud Limited, Rheinsberger Str. 76/77, 10115 Berlin), https://soundcloud.com/pages/privacy
* **Taboola** (Taboola Inc. (28 West 23 St. 5 fl., New York, NY 10010, USA), https://www.taboola.com/privacy-policy

**20. Personalisierte Inhalte**

Zu dem Zweck und in unserem Interesse, unser Angebot für Sie interessanter zu gestalten, verarbeiten wir Informationen zu Ihrem Nutzungsverhalten oder andere historische Nutzungsdaten, einschließlich der früheren Aktivitäten, der Interessen, den Besuchen auf Webseiten oder der Verwendung von Anwendungen, des Standorts oder demografischen Informationen, um Ihnen entsprechend dieser Informationen ausgewählte Inhalten ausspielen zu können. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. f DSGVO. Sie haben jederzeit die Möglichkeit, der Datenverarbeitung zu diesen Zwecken in den Einstellungen der Privatsphäre zu widersprechen.

Vorbehaltlich Ihrer Einwilligung bedienen wir uns dabei auch der Dienste der nachfolgend aufgeführten Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Rechtsgrundlage der Datenverarbeitung ist in diesen Fällen Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Weitere Informationen zur Datenverarbeitung durch die Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* + - **Dutyfarm-Games** Dutyfarm GmbH, Hauptstraße 6b, 10317 Berlin, Deutschland), <https://www.dutyfarm.com/de/impressum/>
    - **Google+** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Google Maps** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Google reCaptcha** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Instagram** (Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland) <https://www.instagram.com/legal/privacy/>
    - **LinkedIn** (LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Irland) <https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy>
    - **SoundCloud**(SoundCloud Limited, Rheinsberger Str. 76/77, 10115 Berlin), https://soundcloud.com/pages/privacy
    - **Taboola** (Taboola Inc. (28 West 23 St. 5 fl., New York, NY 10010, USA), https://www.taboola.com/privacy-policy
    - **Twitter** (Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA), https://twitter.com/de/privacy
    - **Wetterkontor** (Wetterkontor GmbH, Gartenfeldstraße 2, D-55218 Ingelheim), https://www.wetterkontor.de/de/datenschutzhinweise.asp
    - **Youtube** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), https://support.google.com/youtube/answer/7671399?p=privacy\_guidelines&hl=de&visit\_id=0-636644030056539000-341535836&rd=1

**21. Messung der Anzeigen-Leistung**

Vorbehaltlich Ihrer Einwilligung setzen wir Dienste ein zu dem Zweck, die Anzeigen-Leistung zu messen. Diese Dienste messen u.a., ob und wie Anzeigen bei einem Nutzer eingeblendet wurden und wie dieser mit ihnen interagiert hat, ob eine Anzeige in einem ungeeigneten redaktionellen Umfeld (brand-unsafe) eingeblendet wird und bestimmen, zu welchem Prozentsatz die Anzeige hätte wahrgenommen werden können, einschließlich der Dauer (Werbewahrnehmungschance). Sie erstellen zudem Berichte über Anzeigen, einschließlich ihrer Wirksamkeit und Leistung, über die Interaktion von Nutzern mit Anzeigen, und zwar anhand von Daten, die im Laufe der Interaktion des Nutzers mit dieser Anzeige gemessen wurden. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Wir bedienen uns auch der Dienste der nachfolgend aufgeführten Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch die Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* **AdDefend** (AdDefend GmbH, Borselstrasse 3, 22765 Hamburg), <https://www.addefend.com/de/datenschutzerklarung/>
* **AWIN**AWIN AG, Stralauer Allee 2, 10245 Berlin, Deutschland), https://www.awin.com/de/rechtliches/privacy-policy
* **Bing Ads** (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), https://privacy.microsoft.com/de-de/privacystatement
* **Facebook Conversion Pixel** (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), https://www.facebook.com/about/privacy/your-info/
* **Facebook Website Custom Audiences** (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), <https://www.facebook.com/about/privacy/your-info/>
* **Google Ads** (ehem. AdWords) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
* **Google AdSense** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
* **Google Dynamic Remarketing** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
* **Google Floodlight** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
* **Google Marketing Plattform** (ehem. DoubleClick) (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy](http://www.google.de/intl/de/policies/privacy)
* **Sportal**(SPORTAL GmbH Beta-Straße 9a, 85774 Unterföhring Deutschland), <http://www.sportal.de/service/impressum/>
* **Xandr** (ehemals AppNexus)-(Xandr Inc., 28 W. 23rd Street, New York, New York, 10010, USA ) https://www.xandr.com/privacy/platform-privacy-policy/#choicesContact Impact GmbH

**22. Inhaltemessung**

Vorbehaltlich Ihrer Einwilligung setzen wir Dienste ein zu dem Zweck, die Leistung von Inhalten unseres Angebots zu messen. Hierbei wird gemessen und in einem Report dargestellt, wie Inhalte an Nutzer ausgeliefert werden und wie diese mit ihnen interagiert haben. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Wir bedienen uns auch der Dienste der nachfolgend aufgeführten Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch die Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* + - **AGOF** (agof – Arbeitsgemeinschaft Online Forschung e.V. Europa-Allee 22 60327 Frankfurt, Deutschland), <https://www.agof.de/datenschutz/>
    - **Dutyfarm-Games** (Dutyfarm GmbH, Hauptstraße 6b, 10317 Berlin, Deutschland), https://www.dutyfarm.com/de/impressum/
    - **Facebook**(Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), <https://www.facebook.com/about/privacy/your-info/>
    - **Facebook Conversion Pixel** (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), https://www.facebook.com/about/privacy/your-info/
    - **Facebook Website Custom Audiences** (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), <https://www.facebook.com/about/privacy/your-info/>
    - **Google+** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), www.google.de/intl/de/policies/privacy/
    - **Google Maps** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), [www.google.de/intl/de/policies/privacy/](http://www.google.de/intl/de/policies/privacy/)
    - **Instagram** (Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland) <https://www.instagram.com/legal/privacy/>
    - **LinkedIn** (LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Irland) https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic\_footer-privacy-policy
    - **SoundCloud**(SoundCloud Limited, Rheinsberger Str. 76/77, 10115 Berlin), <https://soundcloud.com/pages/privacy>
    - **Sportal**(SPORTAL GmbH Beta-Straße 9a, 85774 Unterföhring Deutschland), <http://www.sportal.de/service/impressum/>
    - **Twitter** (Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA), <https://twitter.com/de/privacy>
    - **VG Wort (**Verwertungsgesellschaft WORT, Rechtsfähiger Verein kraft Verleihung, Untere Weidenstraße 5, 81543 München, Deutschland), https://www.vgwort.de/hilfsseiten/datenschutz.html
    - **Wetterkontor** (Wetterkontor GmbH, Gartenfeldstraße 2, D-55218 Ingelheim), https://www.wetterkontor.de/de/datenschutzhinweise.asp
    - **Youtube** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), https://support.google.com/youtube/answer/7671399?p=privacy\_guidelines&hl=de&visit\_id=0-636644030056539000-341535836&rd=1

**23. Marktforschung (Erkenntnisse über Zielgruppen)**

Vorbehaltlich Ihrer Einwilligung setzen wir Dienste ein zu dem Zweck, Erkenntnisse über Zielgruppen von Werbung und Inhalten zu erzielen. Hierbei werden aggregierte Berichte für Werbetreibende oder deren Repräsentanten über die Zielgruppen, die durch ihre Anzeigen erreicht werden, und welche auf der Grundlage von Befragungspanels oder ähnlichen Verfahren gewonnen wurden, erstellt. Ferner werden aggregierte Berichte für Diensteanbieter über die Zielgruppen, die durch die Inhalte und/oder Anzeigen auf ihren Diensten erreicht wurden bzw. mit diesen interagiert haben, und welche über Befragungspanels oder ähnliche Verfahren ermittelt wurden, erstellt. Die Berichte ermöglichen dabei keinen Rückschluss auf eine bestimmte oder bestimmbare Person. Zur Erstellung dieser Berichte werden jedoch Informationen über Ihr Nutzungsverhalten verarbeitet. Darüber hinaus werden für Zwecke der Marktforschung Offline-Daten zu einem Online-Benutzer zugeordnet, um Erkenntnisse über Zielgruppen zu gewinnen, soweit Anbieter erklärt haben, Offline-Datenquellen abzugleichen und zusammenzuführen. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Wir bedienen uns auch der Dienste der nachfolgend aufgeführten Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch die eingesetzten Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* + - **AGOF** (agof – Arbeitsgemeinschaft Online Forschung e.V. Europa-Allee 22 60327 Frankfurt, Deutschland), <https://www.agof.de/datenschutz/>
    - **Bing Ads** (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), https://privacy.microsoft.com/de-de/privacystatement

**24. Produktentwicklung und -verbesserung**

Vorbehaltlich Ihrer Einwilligung setzen wir Dienste ein zu dem Zweck, Produkte zu entwickeln und zu verbessern, z.B. durch neue Funktionen. Hierfür werden Informationen über Ihr Nutzungsverhalten verarbeitet. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Wir bedienen uns auch der Dienste der nachfolgend aufgeführten Drittanbieter, die gemäß Art. 4 Nr. 7 DSGVO für die über den Dienst stattfindende Datenverarbeitung verantwortlich sind. Weitere Informationen zur Datenverarbeitung durch die Drittanbieter und Ihren Rechten als betroffene Person können Sie den nachfolgend verlinkten Datenschutzerklärungen dieser Drittanbieter entnehmen:

* + - **AGOF** (agof – Arbeitsgemeinschaft Online Forschung e.V. Europa-Allee 22 60327 Frankfurt, Deutschland), <https://www.agof.de/datenschutz/>
    - **Bing Ads** (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), https://privacy.microsoft.com/de-de/privacystatement
    - **Xandr** (ehemals AppNexus)-(Xandr Inc., 28 W. 23rd Street, New York, New York, 10010, USA ) https://www.xandr.com/privacy/platform-privacy-policy/#choicesContact Impact GmbH

**25. Google Werbeanzeigen**

Vorbehaltlich Ihrer Einwilligung verwenden wir zum Zwecke der Refinanzierung unseres Angebots und um Ihnen relevante und personalisierte Werbung aus dem Google Werbenetzwerk anzuzeigen Google Technologien der Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland („Google“), die gemäß Art. 4 Nr. 7 DSGVO für die Verarbeitung personenbezogener Daten verantwortlich ist. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. a DSGVO. Sie haben jederzeit die Möglichkeit, eine von Ihnen erteilte Einwilligung in den Einstellungen der Privatsphäre zu widerrufen. Google arbeitet mit diversen Drittanbietern, über die ebenfalls personalisierte Werbung angezeigt werden kann. Ein Auflistung dieser Drittanbieter finden sie unter folgendem Link: https://support.google.com/admanager/answer/9012903

**26. Vermarktung von Online-Werbeplätzen**

Zu dem Zweck, die auf unserer Website ausgespielte Werbung an Ihren Interessen auszurichten sowie zur Refinanzierung unseres Leistungsangebots, lassen wir die Website wird von unserem Werbevermarkter Media Impact GmbH & Co KG (Media Impact) vermarkten..

Vorbehaltlich Ihrer Einwilligung wird mittels des Einsatzes von Cookies oder entsprechender Technologien Ihr Nutzungsverhalten ausgewertet, um die ausgespielte Werbung für Sie zu optimieren und auf Ihre prognostizierten Interessen auszurichten. Weitere Informationen zu den zu diesem Zweck eingesetzten Cookies können Sie der Privatsphäre entnehmen. Sie können eine von Ihnen erteilte Einwilligung jederzeit mit Wirkung für die Zukunft in den Einstellungen der Privatsphäre widerrufen. Für die zu diesem Zweck stattfindende Verarbeitung personenbezogener Daten ist Media Impact oder von ihr eingesetzte Dritte gemäß Art. 4 Nr. 7 DSGVO verantwortlich. Weitere Informationen zu Media Impact und den von ihr eingesetzten Diensten finden Sie unter <https://www.mediaimpact.de/data/uploads/2020/07/2020-07-02_cmp-_-uber-unsere-werbung-002.pdf>

**27. Affiliate-Marketing**

Sofern Sie über einen Werbebanner von einer externen Internetseite auf unsere Website gelangt sind, erhalten wir von dem Betreiber der externen Website („Affiliate“) die Information, dass ein Nutzer über die externe Seite auf unser Angebot gelangt ist. Hierbei handelt es sich um die dem beworbenen Angebot zugeordnete Produkt-ID sowie die Identifikationsnummer des Affiliate (Affiliate-ID) und eine aus einer beliebigen Nummernfolge erstellte Nutzer-ID. Diese Informationen werden von uns in einem Cookie auf Ihrem Endgerät gespeichert. Sollten Sie innerhalb von 30 Tagen das Angebot auf unserer Website bestellen, werden diese Informationen mit Abschluss des Bestellvorgangs automatisiert und verschlüsselt an den Affiliate übermittelt. Mit Abschluss des Bestellvorgangs, spätestens aber nach Ablauf von 30 Tagen wird der Cookie automatisch gelöscht. Die Verarbeitung dieser Daten erfolgt zu dem Zweck und in dem Interesse, Provisionszahlungen zwischen uns und dem Affiliate abzurechnen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Sie können das Setzen des Cookies wie vorstehend beschrieben durch entsprechende Einstellungen in Ihrem Browser verhindern. Der Affiliate kann anhand der Informationen nur erkennen, dass ein Nutzer von der externen Internetseite über den Werbebanner auf unsere Website gelangt ist und dort das beworbene Produkt bestellt hat. Informationen zur Verarbeitung personenbezogener Daten durch den Affiliate entnehmen Sie bitte den Datenschutzhinweisen des Affiliate auf seiner Internetseite. Entsprechendes gilt, wenn Sie von einem auf unserer Website geschalteten Werbebanner eines Drittanbieters („Advertiser“) auf die Website des Advertiser geleitet werden.

Zudem bedienen wir uns auch der Dienste sog. Affiliate-Netzwerke. Dabei wird ein Cookie auf Ihrem System abgelegt. Was Cookies sind, wurde oben bereits erläutert. Gespeichert werden dabei die Affiliate-ID, sowie die Nutzer-ID und die Produkt-ID. Zweck der Speicherung dieser Daten ist die Abwicklung von Provisionszahlungen zwischen dem Advertiser und uns als Affiliate, welche über das Affiliate-Netzwerk abgewickelt werden. Sie können die Setzung von Cookies durch unsere Website, wie oben bereits dargestellt, jederzeit mittels einer entsprechenden Einstellung des genutzten Internetbrowsers verhindern und damit der Setzung von Cookies dauerhaft widersprechen.

Weitergehende Informationen zu den einzelnen Affiliate-Netzwerken finden Sie in deren jeweiliger Datenschutzerklärung:

* **AWIN** (AWIN AG, Stralauer Allee 2, 10245 Berlin, Deutschland <https://www.awin.com/de/rechtliches/privacy-policy>

**28. Facebook Fanpages**

Wir nutzen unter den folgenden Links Facebook Fanpages, für die wir gemeinsam mit Facebook Ireland Limited verantwortlich sind:

[Eine Liste der WELT-Facebook-Fanpages finden Sie hier.](https://www.welt.de/bin/Facebook-Pages_WELT.pdf_bn-187523902.pdf)

In gemeinsamer Verantwortlichkeit mit Facebook analysieren wir, wie Sie unsere Fanpage nutzen (Seiten-Insights). Die nach der DSGVO erforderlichen Informationen zu der Datenverarbeitung im Rahmen von Seiten-Insights erhalten Sie bei Facebook; derzeit namentlich in den Datenschutzhinweisen von Facebook unter <https://www.facebook.com/legal/terms/information_about_page_insights_data>

Facebook stellt Ihnen auch die relevanten Inhalte des zwischen Facebook und uns geschlossenen Vertrags über die Verarbeitung in gemeinsamer Verantwortlichkeit nach Art. 26 DSGVO zur Verfügung; derzeit unter dem folgenden Link: <https://www.facebook.com/legal/terms/page_controller_addendum>.

Sie können Ihr Beschwerderecht bei jeder für Sie zuständigen Aufsichtsbehörde geltend machen und dort Rechtsbehelfe einlegen.

**Gemäß DSGVO haben Sie ein Recht auf**[**Widerspruch**](https://www.facebook.com/help/contact/1638046109617856)**gegen die Verarbeitung Ihrer Daten. In den oben verlinkten Datenschutzhinweisen von Facebook erfahren Sie mehr über diese und andere Betroffenenrechte.**Für Seiten-Insights auf unseren Facebook Fanpages fungiert Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Irland als gemeinsame Anlaufstelle und bearbeitet sämtliche Anträge zur Geltendmachung der Betroffenenrechte.

Im Rahmen der Seiten-Insights erhalten wir selbst nur anonymisierte Statistiken – auf personenbezogene Daten, die durch Facebook verarbeitet werden, haben wir keinen Zugriff. Die Verarbeitung der anonymisierten Daten durch uns erfolgt auf Basis gesetzlicher Vorschriften, die es uns gestatten, personenbezogene Daten zu verarbeiten, weil wir ein überwiegendes berechtigtes Interesse daran haben, ein besseres Verständnis der Interessen der Besucher unserer Fanpage zu erlangen (Art. 6 Abs. 1 f) DSGVO). Facebook bietet auf den Fanpages verschiedene Community-Funktionen an, mit denen Sie mit anderen Nutzern in Interaktion treten können, etwa indem Sie dort Beiträge posten, Kommentare hinterlassen oder Beiträge liken bzw. teilen können. Wir weisen darauf hin, dass diese Bereiche öffentlich zugänglich sind und sämtliche persönlichen Informationen, die Sie darin einstellen oder bei der Anmeldung bereitstellen, von anderen eingesehen werden können. Wir können nicht kontrollieren, wie andere Nutzer der Fanpages diese Informationen verwenden. Insbesondere können wir nicht verhindern, dass unerwünschte Nachrichten an Sie gesendet werden.

**29.Social Plugins**

Auf dieser Website sind keine Social Media Plugins integriert, die direkt Daten von den Servern der betreffenden Social Media-Anbieter laden. Bei den integrierten „Plugins“ handelt es sich vielmehr um einfache Links zu den betreffenden Drittseiten, die wir mit entsprechend Grafiken bebildern. Eine Übermittlung personenbezogener Daten an den Betreiber des Social Media-Dienstes durch die bekannten Plugins findet daher nicht statt.

**30. Augmented Reality**

Zu dem Zweck und in unserem Interesse, das Nutzungserlebnis unserer Angebote zu steigern, setzen wir Augmented Reality ein. Wir bedienen uns dabei der Dienste der 8th Wall, Inc., 250 Cambridge Ave, Suite 101, Palo Alto, CA 94306 („8th Wall“), mit denen wir eine datenschutzrechtliche Vereinbarung (Art. 28, 46 DSGVO) getroffen haben. Verantwortlich für die Datenverarbeitung bleiben wir. Sofern Sie den Dienst nutzen, verarbeitet 8th Wall in unserem Auftrag Ihre IP-Adresse, Informationen über das zugreifende Endgerät und die verwendete Software sowie Datum und Uhrzeit des Zugriffs. Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b DSGVO. Die Nutzung des Dienstes erfordert zudem den Zugriff auf die Kamera Ihres Endgeräts. Rechtsgrundlage hierfür ist Art. 6 Abs. 1 lit. a DSGVO. Den Zugriff auf die Kamera können Sie jederzeit in den Einstellungen Ihres Endgeräts deaktivieren und damit eine von Ihnen erteilte Einwilligung widerrufen.“

**31. Partnerangebote**

In unsere Website sind Angebote von Partnern integriert („Partnerangebote“). Sie erkennen diese an der entsprechenden Kennzeichnung (z.B. „Ein Angebot von“). Die Partnerangebote werden von dem dort angegebenen Partner bereitgestellt. Hierbei erheben wir keinerlei personenbezogenen Daten noch übermitteln wir diese an den Partner. Für das Ausspielen der Partnerangebote ist es erforderlich, dass Ihr Browser eine direkte Verbindung zu den Servern des Partners aufbaut. Hierfür ist die Verarbeitung Ihrer IP-Adresse erforderlich. Verantwortlich für die darüber hinaus über das Partnerangebot stattfindenden Datenverarbeitungsvorgänge gemäß Art. 4 Nr. 7 DSGVO ist der Partner. Informationen zu den über die Partnerangebote stattfindenden Datenverarbeitungsvorgängen entnehmen Sie bitte der in dem jeweiligen Partnerangebot verlinkten Datenschutzerklärung des Partners.

**32. Integration von Drittanbietern (Soziale Netzwerke)**

Zu dem Zweck , das Nutzungserlebnis in unserem Angebot zu steigern, betten wir auch Dienste der unten aufgelisteten Drittanbieter ein, die gemäß Art. 4 Nr. 7 DSGVO jeweils für die Datenverarbeitung verantwortlich sind. Vorbehaltlich Ihrer Einwilligung baut Ihr Browser eine direkte Verbindung zu dem Server des jeweiligen Drittanbieters auf. Hierbei wird von dem Drittanbieter stets Ihre IP-Adresse verarbeitet, die für den Aufbau der Verbindung zum Server des Drittanbieters und dem Ausspielen der Inhalte erforderlich ist. Rechtsgrundlage für die Einbindung dieser Dienste ist Art. 6 Abs. 1 lit. a DSGVO. Eine von Ihnen erteilte Einwilligung können Sie jederzeit mit Wirkung für die Zukunft in den Einstellungen Ihrer Privatsphäre widerrufen.

Informationen zur Datenverarbeitung durch den jeweiligen Drittanbieter können Sie der Datenschutzerklärung des jeweiligen Drittanbieters entnehmen.

* + - **Dutyfarm-Games** Dutyfarm GmbH, Hauptstraße 6b, 10317 Berlin, Deutschland), <https://www.dutyfarm.com/de/impressum/>
    - **Facebook** (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), <https://www.facebook.com/about/privacy/your-info/>
    - **Facebook Website Custom Audiences** (Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA), https://www.facebook.com/about/privacy/your-info/
    - **Giphy** (Giphy, Inc., 416 W 13th Street Suite 207, New York, NY 10014)  
      <https://giphy.com/privacy>
    - **Instagram** (Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland) <https://www.instagram.com/legal/privacy/>
    - **SoundCloud**(SoundCloud Limited, Rheinsberger Str. 76/77, 10115 Berlin), <https://soundcloud.com/pages/privacy>
    - **Sportal** (SPORTAL GmbH Beta-Straße 9a, 85774 Unterföhring Deutschland), <http://www.sportal.de/service/impressum/>
    - **Traumjob finden / Stepstone** (StepStone Deutschland GmbH, Völklinger Straße 1, 40219 Düsseldorf, Deutschland), <https://www.stepstone.de/Ueber-StepStone/Rechtliche-Hinweise/datenschutzerklaerung/>
    - **Twitter** (Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA), <https://twitter.com/de/privacy>
    - **VG Wort (**Verwertungsgesellschaft WORT, Rechtsfähiger Verein kraft Verleihung, Untere Weidenstraße 5, 81543 München, Deutschland), https://www.vgwort.de/hilfsseiten/datenschutz.html
    - **Wetterkontor** (Wetterkontor GmbH, Gartenfeldstraße 2, D-55218 Ingelheim), https://www.wetterkontor.de/de/datenschutzhinweise.asp
    - **Xandr** (ehemals AppNexus)-(Xandr Inc., 28 W. 23rd Street, New York, New York, 10010, USA ) https://www.xandr.com/privacy/platform-privacy-policy/#choicesContact Impact GmbH
    - **Youtube** (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland), https://support.google.com/youtube/answer/7671399?p=privacy\_guidelines&hl=de&visit\_id=0-636644030056539000-341535836&rd=1

**33. Speicherdauer**

Wir verarbeiten personenbezogene Daten nur solange dies für den jeweils vorstehend genannten Zweck erforderlich ist. Die personenbezogenen Daten werden anschließend gelöscht, sofern einer Datenlöschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

**34. Kontaktdaten und Ihre Rechte als betroffene Person**

Bitte wenden Sie sich bei Fragen und Anregungen zum Datenschutz sowie zur Durchsetzung Ihrer Rechte als betroffene Person jederzeit an unseren Datenschutzbeauftragten:

Axel Springer SE  
Datenschutz  
Axel-Springer-Str. 65  
10888 Berlin  
[datenschutz@welt.de](http://datenschutz@welt.de/)

Soweit es die Datenverarbeitung mit einem gemeinsam Verantwortlichen nach Art. 26 DSGVO erfolgt, agieren beide Verantwortlichen als gemeinsame Anlaufstelle

▫ **Auskunft, Berichtigung, Löschung, Einschränkung und das Recht auf Vergessenwerden**

Sie können von uns jederzeit unentgeltlich Auskunft darüber erhalten, ob personenbezogene Daten zu Ihrer Person von uns verarbeitet werden und auch konkret welche Daten über sie gespeichert werden sowie eine Kopie der gespeicherten Daten verlangen. Sie können ferner unrichtige Daten berichtigen und vervollständigen lassen.

Auch können Sie die Löschung und Einschränkung Ihrer personenbezogenen Daten verlangen. Bitte beachten Sie, dass es z. B. für entgeltliche Verträge wie dem Kauf eines Abonnements von WELT Digital gesetzliche Aufbewahrungspflichten gibt und wir daher Ihre Daten nicht in jedem Fall vollständig löschen dürfen. In diesem Fall werden Ihre Daten mit dem Ziel markiert, ihre künftige Verarbeitung einzuschränken.

Um Auskunft zu erhalten, bzw. zur Löschung Ihrer Daten bitten wir Sie, das unter <https://www.axelspringer.com/de/datenschutzerklaerung/formular-auskunftsersuchen-und-loeschersuchen> abrufbare Dokument auszufüllen. Auf diesem Wege können wir unbürokratisch sicherstellen, dass personenbezogene Daten nur an Sie als berechtigte Personen herausgegeben werden, bzw. von Ihnen gelöscht werden.. Sind Sie mit der Nutzung des Formulars nicht einverstanden, so schreiben Sie uns dies bitte kurz per E-Mail an [datenschutz.kundenservice@axelspringer.de](mailto:datenschutz.kundenservice@axelspringer.de) oder rufen Sie uns an unter (030) 5858 5379. Wir werden dann gemeinsam einen anderen Weg finden, der Ihre Identifizierung sicherstellt.

▫ **Datenübertragbarkeit**

Sofern anwendbar haben Sie außerdem das Recht, dass die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format an Sie oder einen anderen Verantwortlichen übermittelt werden, sofern die Verarbeitung auf der Einwilligung oder einem Vertrag beruht und mithilfe automatisierter Verfahren erfolgt. Dies gilt jedoch nicht, sofern die Verarbeitung nicht für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, welche dem Verantwortlichen übertragen wurde. Ferner haben Sie das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist und sofern hiervon nicht die Rechte und Freiheiten anderer Personen beeinträchtigt werden.

▫ **Widerruf / Widerspruch**

Ihre abgegebenen Einwilligungen können Sie jederzeit mit Wirkung für die Zukunft unter der o. g. Kontaktadresse widerrufen. Insbesondere können Sie der Verwendung Ihrer E-Mail-Adresse zum Zwecke des Newsletterversandes jederzeit schriftlich oder in Textform an [datenschutz@welt.de](http://datenschutz@welt.de/) oder Axel-Springer-Str. 65 in 10888 Berlin mit Wirkung für die Zukunft widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen. Ferner haben Sie das Recht aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund eines berechtigten oder öffentlichen Interesses erfolgt, Widerspruch einzulegen. Dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Wir verarbeiten die personenbezogenen Daten im Falle des Widerspruchs nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Sofern wir personenbezogene Daten verarbeiten, um Direktwerbung zu betreiben, so haben Sie das Recht, jederzeit Widerspruch gegen die Verarbeitung der personenbezogenen Daten zum Zwecke derartiger Werbung unter der. o. g. Kontaktadresse einzulegen. Dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Zudem haben Sie das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Sie betreffende Verarbeitung personenbezogener Daten, die bei uns zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgen, Widerspruch einzulegen, es sei denn, eine solche Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

▫ **Beschwerderecht**

Ferner haben Sie ein Beschwerderecht bei der zuständigen Aufsichtsbehörde sowie die Möglichkeit Rechtsbehelfe einzulegen. Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs.

▫ **Bestehen einer automatisierten Entscheidungsfindung**

Wir verzichten auf eine automatische Entscheidungsfindung oder ein Profiling im Sinne des Art. 22 DSGVO.

**Stand:** 17. September 2020

Sofern Sie dies wünschen, schicken wir Ihnen diese Datenschutzerklärung selbstverständlich kostenfrei per Post zu. Bitte kontaktieren Sie uns hierzu unter Axel Springer SE, Betrieblicher Datenschutz, Axel-Springer-Straße 65, 10888 Berlin.

T Online Nachrichten

**Hinweise zum Datenschutz**



**Hinweise zum Datenschutz auf t-online.de**

Wir, die Ströer Digital Publishing GmbH, Platz der Einheit 1, 60327 Frankfurt („**Ströer**“, „**wir**“ oder „**uns**“), freuen uns über Ihren Besuch auf t-online.de. Der Schutz und die Sicherheit Ihrer Daten haben für uns höchste Priorität. Diese Hinweise zum Datenschutz („**Datenschutzhinweise**“) erläutern insbesondere, welche Informationen wir während Ihres Besuchs auf unserer Webseite t-online.de erheben, wie und wofür wir diese Informationen verwenden und mit wem wir diese teilen. Zudem erklären wir Ihnen Ihre Rechte in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten, etwa die Rechte auf Auskunft, Berichtigung, Widerspruch und Löschung.

ÜBERBLICK

* [1. Allgemeines](https://www.t-online.de/datenschutz/id_88397036/index#1._allgemeines)
* [1.1 Wer ist für die Verwendung Ihrer Daten verantwortlich?](https://www.t-online.de/datenschutz/id_88397036/index#1.1_wer_ist_f%C3%BCr_die_verwendung_ihrer_daten_verantwortlich)
* [1.2 Welche Daten erheben wir von Ihnen?](https://www.t-online.de/datenschutz/id_88397036/index#1.2_welche_daten_erheben_wir_von_ihnen)
* [1.3 Einwilligungsmanagement](https://www.t-online.de/datenschutz/id_88397036/index#1.3_einwilligungsmanagement)
* [1.4 Zu welchem Zweck und auf welcher rechtlichen Grundlage erheben wir Ihre Daten?](https://www.t-online.de/datenschutz/id_88397036/index#1.4_zu_welchem_zweck_und_auf_welcher_rechtlichen_grundlage_erheben_wir_ihre_daten)
* [1.5 Mit wem teilen wir Ihre Daten?](https://www.t-online.de/datenschutz/id_88397036/index#1.5_mit_wem_teilen_wir_ihre_daten)
* [1.6 Wo werden Ihre persönlichen Daten verarbeitet?](https://www.t-online.de/datenschutz/id_88397036/index#1.6_wo_werden_ihre_pers%C3%B6nlichen_daten_verarbeitet)
* [1.7 Wie lange behalten wir Ihre Daten?](https://www.t-online.de/datenschutz/id_88397036/index#1.7_wie_lange_behalten_wir_ihre_daten)
* [1.8 Welche Rechte haben Sie hinsichtlich Ihrer Daten?](https://www.t-online.de/datenschutz/id_88397036/index#1.8_welche_rechte_haben_sie_hinsichtlich_ihrer_daten)
* [1.9 Widerspruchsrechte gem. Art. 21 DSGVO](https://www.t-online.de/datenschutz/id_88397036/index#1.9_widerspruchsrechte_gem._art._21_dsgvo)
* [2. Cookies und ähnliche Technologien von t-online.de](https://www.t-online.de/datenschutz/id_88397036/index#2._cookies_und_%C3%A4hnliche_technologien_von_t-online.de)
* [2.1 Cookies](https://www.t-online.de/datenschutz/id_88397036/index#2.1_cookies)
* [2.2 Ähnliche Technologie](https://www.t-online.de/datenschutz/id_88397036/index#2.2_%C3%A4hnliche_technologie)
* [3. Von uns eingesetzte Technologien](https://www.t-online.de/datenschutz/id_88397036/index#3._von_uns_eingesetzte_technologien)
* [3.1 Google-Analytics](https://www.t-online.de/datenschutz/id_88397036/index#3.1_google-analytics)
* [3.2 Google Analytics Remarketing](https://www.t-online.de/datenschutz/id_88397036/index#3.2_google_analytics_remarketing)
* [3.3 Google AdWords und Google Conversion-Tracking](https://www.t-online.de/datenschutz/id_88397036/index#3.3_google_adwords_und_google_conversion-tracking)
* [3.4 Taboola](https://www.t-online.de/datenschutz/id_88397036/index#3.4_taboola)
* [3.5 Civey](https://www.t-online.de/datenschutz/id_88397036/index#3.5_civey)
* [3.6 Conversario](https://www.t-online.de/datenschutz/id_88397036/index#3.6_conversario)
* [3.7 Opinary](https://www.t-online.de/datenschutz/id_88397036/index#3.7_opinary)
* [3.8 Heatmap](https://www.t-online.de/datenschutz/id_88397036/index#3.8_heatmap)
* [3.9 Seeding Alliance](https://www.t-online.de/datenschutz/id_88397036/index#3.9_seeding_alliance)
* [3.10 trbo (www.trbo.com/)](https://www.t-online.de/datenschutz/id_88397036/index#3.10_trbo_(www.trbo.com/))
* [3.11 Criteo (https://www.criteo.com/de)](https://www.t-online.de/datenschutz/id_88397036/index#3.11_criteo_(https//www.criteo.com/de))
* [3.12 SpeedCurve (https://speedcurve.com/)](https://www.t-online.de/datenschutz/id_88397036/index#3.12_speedcurve_(https//speedcurve.com/))
* [4. Technologien von eigenverantwortlichen Dritten](https://www.t-online.de/datenschutz/id_88397036/index#4._technologien_von_eigenverantwortlichen_dritten)
* [4.1 Reichweitenmessung / Webanalyse](https://www.t-online.de/datenschutz/id_88397036/index#4.1_reichweitenmessung_/_webanalyse)
* [4.2 Werbung / Individualisierung](https://www.t-online.de/datenschutz/id_88397036/index#4.2_werbung_/_individualisierung)
* [4.3 Weitere Dienste auf t-online.de / Social Plugins](https://www.t-online.de/datenschutz/id_88397036/index#4.3_weitere_dienste_auf_t-online.de_/_social_plugins)
* [5. Kontakt, Geltendmachung Ihrer Rechte](https://www.t-online.de/datenschutz/id_88397036/index#5._kontakt_geltendmachung_ihrer_rechte)
* [6. Wie oft aktualisieren wir diese Datenschutzhinweise?](https://www.t-online.de/datenschutz/id_88397036/index#6._wie_oft_aktualisieren_wir_diese_datenschutzhinweise)

Wir werden Ihre personenbezogene Daten (im Folgenden: „ **Daten**“) nur in Übereinstimmung mit dem geltenden Datenschutzrecht verwenden. Wenn wir Ihre Daten für andere als die in diesem Datenschutzhinweis angegebenen Zwecke verwenden, werden wir Sie über diese Zwecke informieren und soweit erforderlich Ihre Einwilligung einholen.

Die rechtlichen Grundlagen, auf die wir uns für unsere Datenverarbeitung stützen, finden Sie zum Großteil in der Datenschutzgrundverordnung („**DSGVO**“), die Sie z.B. [hier](https://dsgvo-gesetz.de/) abrufen können. In den nachfolgend dargestellten Datenschutzhinweisen verweisen wir auch auf die entsprechenden Rechtsgrundlagen unserer Verarbeitung.

**1. Allgemeines**

**1.1 Wer ist für die Verwendung Ihrer Daten verantwortlich?**

Ströer ist verantwortliche Stelle im Sinne des anwendbaren Datenschutzrechts. Das bedeutet, dass wir für die Verwendung Ihrer von uns erhobenen Daten verantwortlich und gesetzlich verpflichtet sind, sicherzustellen, dass die erforderlichen Maßnahmen zum Schutz Ihrer Daten getroffen und Ihre Rechte gewahrt werden.

**1.2 Welche Daten erheben wir von Ihnen?**

Abhängig von den Informationen, die Sie uns zur Verfügung stellen, erfassen wir folgende Daten:

* Daten über die Nutzung unserer Dienste
* Wir erfassen Informationen über Sie, wenn Sie unsere Dienste nutzen, sich z.B. einen Artikel oder ein Video ansehen. Dabei handelt es sich um folgende Daten:

**- Gerätebezogene Informationen**  
Wir erfassen gerätespezifische Informationen, beispielsweise das Modell der von Ihnen verwendeten Hardware, die Version des Betriebssystems, eindeutige Gerätekennungen und Informationen über das Mobilfunknetz, Daten zu Geräteereignissen wie Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit Ihrer Anfrage und Referral-URL.

**- Ihre IP-Adresse**

**- Standortbezogene Informationen**  
Wenn Sie unsere Dienste nutzen, erfassen und verarbeiten wir möglicherweise Informationen über Ihren Standort. Wir verwenden zur Standortbestimmung verschiedene Technologien, wie IP-Adressen, GPS und andere Sensoren, die uns beispielsweise Informationen über nahe gelegene Geräte, WLAN-Zugangspunkte oder Mobilfunkmasten bereitstellen. Standortdaten verarbeiten wir nur mit Ihrer Zustimmung. Die Erfassung von Standortdaten können Sie über unseren Privacy Manager und in den Einstellungen Ihres Mobilgeräts jederzeit kontrollieren, aktivieren oder deaktivieren.

**- Cookies**  
Wenn Sie unsere Webseite t-online.de besuchen, sammeln wir Informationen über Sie, indem wir Cookies einsetzen. Hierfür bitten wir Sie – soweit dies gesetzlich erforderlich ist – in unserem Privacy Manager um Ihre Einwilligung.

Cookies sind kleine Textdateien, die eine Wiedererkennung Ihres Browsers ermöglichen. Wir verwenden Cookies, um Ihnen eine nutzerfreundliche und sichere Webseite anbieten zu können und unsere Dienste an Ihre Bedürfnisse und Interessen anzupassen, z.B. indem wir Ihr Browser-Erlebnis individualisieren oder Ihnen auf Sie zugeschnittene Werbung anzeigen (weitergehende Informationen zu Cookies finden Sie in unserem Privacy Manager und unter Ziffer 2 (Verlinken)

**- Umfragen, Werbeaktionen und Gewinnspiele**  
Von Zeit zu Zeit geben wir Ihnen die Möglichkeit, an Umfragen oder Gewinnspielen teilzunehmen. Wenn Sie sich freiwillig beteiligen, werden wir unter Umständen zusätzliche Daten von Ihnen erfragen und verarbeiten (z.B. Ihre Anschrift zum Zweck der Gewinnbenachrichtigung sowie E-Mail-Adresse und Telefonnummer, um eine Gewinnbenachrichtigung auch im Falle versehentlich fehlerhafter Adressangaben sicherstellen zu können, und das Geburtsdatum zum Zweck der Altersprüfung). Eine weitergehende Nutzung Ihrer Daten, etwa zum Zwecke der Veröffentlichung des Gewinners auf unserer Plattform, geschieht nur mit Ihrer ausdrücklichen Zustimmung.

**- Newsletter**  
Wenn Sie sich durch Ihre Einwilligung freiwillig bei unserem Newsletter registrieren, erfassen wir die von Ihnen angegebene E-Mail-Adresse, sowie Ihren Vor- und Nachnamen. Sie haben jederzeit die Möglichkeit, die Zusendung von Newslettern zu beenden. Hierzu folgen Sie einfach dem Link zum Abbestellen des Newsletters am Ende der jeweiligen Nachricht oder wenden sich an die unter Ziffer 5 angegebenen Kontaktdaten.

**- Daten über Ihre Sozialen Netzwerk Dienste**

a) Login über Soziale Netzwerk Dienste  
Sofern Sie Soziale Netzwerk Dienste („SND“) für eine Registrierung auf unserer Seite nutzen möchten und bei diesen angemeldet sind, werden Sie aufgefordert, sich beim SND einzuloggen. Hierbei ist für uns weder Ihr Benutzername oder Ihr Passwort sichtbar, noch werden wir diese Daten speichern oder sonst in irgendeiner Weise verwenden. Wir lassen uns vom entsprechenden SND nur einen Authentifizierungs-Token übergeben. Wenn Sie nicht möchten, dass die Social Media Netzwerke Daten über Sie über unsere Seite sammeln, sollten Sie diese nicht für einen Login auf unserer Seite verwenden.

b) Social Plugins

Auf t-online.de finden Sie Buttons von den unter Ziffer 4.3 aufgeführten Sozialen Netzwerk Diensten („SND“). Nähere Informationen zu Zweck und Umfang der Verarbeitung Ihrer Daten sowie Einstellungsmöglichkeiten zum Schutz Ihrer Privatsphäre können Sie zum einen den Angaben unter Ziffer 4.3 und zum anderen den Datenschutzrichtlinien des jeweiligen SND entnehmen.

Grundsätzlich sind Sie nicht dazu verpflichtet, uns Ihre Daten zur Verfügung zu stellen. Die Nutzung bestimmter Funktionen kann allerdings die Angabe personenbezogener Daten erfordern, z. B. das Abonnement eines Newsletters. Wenn dies der Fall ist, weisen wir Sie darauf hin. Wenn Sie uns die hierfür erforderlichen Daten nicht zur Verfügung stellen möchten, können Sie die entsprechenden Funktionen leider nicht nutzen.

**1.3 Einwilligungsmanagement**

Wir bieten Ihnen mit dem Privacy Manager die Möglichkeit, selbst detailliert entscheiden zu können, in welchen Fällen Sie Tracking via Cookies und anderer Technologien - insbesondere zwecks Anzeige für Sie relevanter Inhalte sowie auf Sie maßgeschneiderter Werbung - zustimmen wollen.  
  
Die Verarbeitung Ihrer Daten zu oben genannten Zwecken erfolgt teilweise auf der Grundlage des berechtigten Interesses, teilweise benötigen wir jedoch auch Ihre Zustimmung.  
  
Um die Anforderungen der Datenschutzgrundverordnung (DSGVO) zu gewährleisten und ein Höchstmaß an Transparenz für Sie als Nutzer bereit zu stellen, nehmen wir am Transparency & Consent Framework (TCF) von IAB Europe teil und unterwerfen uns dessen Spezifikationen und Richtlinien. Dafür setzen wir die Consent-Management-Plattform (CMP) der Sourcepoint Technologie Inc., 228 Park Ave S #87903, New York 10003-1502, USA („Sourcepoint“) als Auftragsverarbeiter ein. Im Rahmen des IAB Europe Transparency & Consent Frameworks ist Sourcepoint unter der Identifikationsnummer 6 gelistet. Die CMP von Sourcepoint ermöglicht es Ihnen, uns eine datenschutzkonforme und selbstbestimmte Einwilligung in die Verarbeitung Ihrer Daten zu erteilen sowie diese jederzeit zu widerrufen. Auch können Sie der Datenverarbeitung widersprechen, die auf unserem berechtigten Interesse beruht.  
  
Eine Übersicht Ihrer Einstellungsmöglichkeiten, den Zwecken und eingebundenen Dritten finden Sie hier: Privacy Manager  
  
Weitere Informationen zum Datenschutz und der CMP von Sourcepoint finden Sie auf der Website [www.sourcepoint.com/privacy-policy.](https://www.sourcepoint.com/privacy-policy)  
Darüber hinaus können Sie sich auf der Website von IAB Europe über das Transparency and Consent Framework (TCF) informieren: [iabeurope.eu/](https://iabeurope.eu/)

**1.4 Zu welchem Zweck und auf welcher rechtlichen Grundlage erheben wir Ihre Daten?**

Wir nutzen Ihre Daten auf Grundlage:

* Ihrer Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a, Art. 7 DSGVO

- zur Produktinformation oder -beratung (beispielsweise das Zusenden personalisierter Werbung), beispielsweise durch unseren Newsletter, oder Gewinnspiele

- um Ihnen maßgeschneiderte Inhalte anzubieten, beispielsweise, um Ihnen relevantere Suchergebnisse und personalisierte Werbung zur Verfügung zu stellen

* der Erfüllung des Vertrages, dessen Vertragspartei Sie sind, oder zur Erfüllung vorvertraglicher Pflichten Ihnen gegenüber gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO

- zur Ermöglichung der Nutzung unserer Dienste durch das Teilen von Beiträgen und Interessen, Vorlieben und Gedanken auf unserer Website  
- zur Übermittlung von Mitteilungen zur Nutzung unserer Dienste, einschließlich Mitteilungen zu anstehenden Veränderungen oder Verbesserungen, an Ihre E-Mail-Adresse  
- zur Behebung sonstiger Probleme hinsichtlich unserer Dienste und der Speicherungen unserer Kommunikation mit Ihnen dazu, soweit dies für die Problembeseitigung erforderlich ist  
- zur Durchsetzung geltender Nutzungsbedingungen (z.B. bei Verzögerungen der Erfüllung des Vertrags)

* unserer berechtigten Interessen gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO

- zur Bereitstellung, zur Wartung, zum Schutz und zur Verbesserung unserer Dienste, zur Entwicklung neuer Dienste sowie zu unserem Schutz und zum Schutz unserer Nutzer, außerdem, um Ihnen maßgeschneiderte Inhalte anzubieten, beispielsweise, um Ihnen relevantere Suchergebnisse und personalisierte Werbung zur Verfügung zu stellen  
- zur weiteren Verbesserung der Sicherheit unseres IT-Systems zum Vorteil aller Nutzer  
- zur Kommunikation mit Ihnen  
- zur Aufdeckung, zur Verhinderung oder zur Bekämpfung von Rechtsverstößen  
- zur Aufdeckung, zur Verhinderung oder zur Behebung von Sicherheitsmängeln oder technischen Problemen  
- zum Schutz von Rechten, die das Eigentum oder die Sicherheit von Ströer, unserer Nutzer oder der Öffentlichkeit betreffen  
- zur Durchsetzung geltender Nutzungsbedingungen , einschließlich der Untersuchung möglicher Verstöße gegen die Nutzungsbedingungen oder das geltende Recht (z.B. Beleidigungen, Betrug)  
- zum Schutz von Rechten, die das Eigentum oder die Sicherheit von Ströer, unserer Nutzer oder der Öffentlichkeit betreffen, soweit gesetzlich zulässig und erforderlich

* gesetzlicher Verpflichtungen gem. Art. 6 Abs. 1 S. 1 lit. c DSGVO

- zur Erfüllung und Einhaltung von geltenden Gesetzen, Vorschriften oder Rechtsverfahren oder einer vollstreckbaren behördlichen Anordnung  
- zur Aufdeckung, zur Verhinderung oder zur Bekämpfung von Rechtsverstößen, sofern Ströer hierzu gesetzlich verpflichtet ist oder Dritte darauf einen gesetzlichen Anspruch gegenüber Ströer haben.  
- zur Aufdeckung, zur Verhinderung oder zur Behebung von Sicherheitsmängeln oder technischen Problemen

**1.5 Mit wem teilen wir Ihre Daten?**

Wir geben keine Daten an Unternehmen, Organisationen oder Personen außerhalb von Ströer weiter, außer:

* **Mit Ihrer Einwilligung**  
  Wir geben Daten an Unternehmen, Organisationen oder Personen außerhalb von Ströer weiter, wenn wir hierfür Ihre Einwilligung erhalten haben.
* **Für die Verarbeitung durch andere Stellen (im Auftrag)**  
  .Wir stellen Daten unseren Partnern, anderen vertrauenswürdigen Unternehmen oder Personen zur Verfügung, die diese in unserem Auftrag verarbeiten („Auftragsverarbeitung“). Dies geschieht auf der Grundlage unserer Weisungen und im Einklang mit dem geltendem Recht, sowie geeigneten Vertraulichkeits- und Sicherheitsmaßnahmen, mit denen wir jederzeit den Schutz Ihrer Daten sicherstellen.
* **Aus rechtlichen Gründen**

Wir werden Daten an Unternehmen, Organisationen oder Personen außerhalb von Ströer weitergeben, wenn wir nach Treu und Glauben davon ausgehen dürfen, dass der Zugriff auf diese Daten oder ihre Nutzung, Aufbewahrung oder Weitergabe notwendig ist, um  
- geltende Gesetze, Vorschriften oder Rechtsverfahren einzuhalten oder einer vollstreckbaren behördlichen Anordnung nachzukommen  
- Betrug, Sicherheitsmängel oder technische Probleme aufzudecken zu verhindern oder anderweitig zu bekämpfen  
- die Rechte, das Eigentum oder die Sicherheit von Ströer, unserer Nutzer oder der Öffentlichkeit vor Schaden zu schützen, soweit gesetzlich zulässig oder erforderlich

* **Für die anonyme Verarbeitung durch andere Stellen**  
  Wir geben möglicherweise nicht personenbezogene Daten, d.h. solche Daten, bei denen kein Rückschluss auf eine konkrete Person möglich ist, an die Öffentlichkeit und unsere Partner weiter, beispielsweise an andere Werbetreibende oder verbundene Websites. So veröffentlichen wir zum Beispiel Informationen, um Trends bei der allgemeinen Nutzung unserer Dienste aufzuzeigen.

In den in diesem Abschnitt genannten Fällen können Ihre personenbezogenen Daten an folgende Kategorien von Empfängern weitergegeben werden:  
- IT-Dienstleister (technischer Support),  
- IT-Dienstleister (Data Hosting Provider),  
- Kundensupport (E-Mail, Telefon),  
- Behörden, Gerichte, Rechtsanwälte, Wirtschaftsprüfer, Steuerberater  
Soweit wir mit Hilfe von Webanalysetools Daten erheben bzw. erheben lassen und Webwerbe-Tools verwenden und in diesem Zusammenhang mit eigenverantwortlichen Dritten (die nicht Auftragnehmer einer Auftragsverarbeitung sind) zusammenarbeiten, informieren wir Sie hierüber in unserem Privacy Manager. Weitere Details zu Tools finden Sie außerdem unter Ziff. 3. Dort erhalten Sie auch jeweils die Information, wie Sie Ihr Recht auf Widerspruch gegen Datenverarbeitungen auf Basis unserer berechtigten Interessen (Opt-Out) ausüben können und welche technischen Möglichkeit Sie haben, um Datenerhebungen von vornherein zu verhindern.

**1.6 Wo werden Ihre persönlichen Daten verarbeitet?**

Ihre personenbezogenen Daten werden sowohl innerhalb als auch außerhalb der Europäischen Union („ EU“) und des Europäischen Wirtschaftsraums („ EWR“) durch uns oder von den in Ziffer 1.5 genannten Parteien verarbeitet. Bitte beachten Sie: Wenn Ihre Daten von Ihrem Heimatland in ein anderes Land übermittelt werden, können die dortigen Gesetze zum Schutz Ihrer Daten von denen Ihres Landes abweichen (und gegebenenfalls nur ein geringeres Schutzniveau gewährleisten). Beispielsweise gelten insbesondere in Ländern außerhalb des EWR andere Voraussetzungen, unter denen Strafverfolgungsbehörden Zugriff auf Ihre Daten nehmen können, als innerhalb des EWR. Sofern wir Ihre Daten in ein Land außerhalb des EWR übermitteln, werden wir geeignete Maßnahmen treffen, um ein angemessenes Datenschutzniveau sicherzustellen (etwa durch den Abschluss von Standardvertragsklauseln).  
Sie haben das Recht, eine Kopie der konkret vereinbarten Regelungen zur Sicherstellung des angemessenen Datenschutzniveaus zu erhalten. Bitte nutzen Sie hierfür die Angaben unter Ziffer 5.

**1.7 Wie lange behalten wir Ihre Daten?**

Wir werden Ihre Daten nicht länger als zur Erfüllung des jeweiligen Zwecks, für den sie erhoben wurden bzw. solange wir ein berechtigtes Interesse an der Speicherung haben und dieses Interesse Ihr Interesse an der Löschung überwiegt speichern, es sei denn, für eine längere Speicherung besteht eine gesetzliche Grundlage (z.B. auch aufgrund Handels- oder Steuerrecht gem. Art. 6 Abs. 1 Satz 1 lit. c DSGVO. Bei einer solchen Archivierung werden die Daten für sonstige Zugriffe gesperrt und nach Ablauf der gesetzlichen Aufbewahrungsfristen datenschutzgerecht gelöscht und vernichtet). Anschließend werden wir Ihre Daten löschen. Die jeweiligen Aufbewahrungsfristen sind von dem zugrundeliegenden Zweck und von der Art der Daten abhängig.  
Insbesondere behalten wir

* Daten, die wir für personalisierte Werbung verwenden (etwa Ihre E-Mail-Adresse, wenn Sie sich für unseren Newsletter registrieren) für einen Zeitraum von bis zu 12 Monaten ab dem Zeitpunkt, zu dem wir Sie das letzte Mal kontaktierten, es sei denn, Sie verlangen eine vorherige Löschung und es liegen keine gesetzlichen Speicherpflichten vor
* Ihre IP-Adresse für maximal 10 Tage
* Cookies, die keine sog. Session Cookies sind, in der Regel für einen Zeitraum von 12 Monaten, maximal aber für 36 Monate. Darüber hinaus können Sie Cookies jederzeit von Ihrem Computer löschen oder Ihre ggf. erteilte Einwilligung in die Verwendung von Cookies in unserem Privacy Manager widerrufen.
* Daten, die Sie auf unserer Plattform teilen, solange Sie Ihren Account nutzen.
* Daten aus Umfragen, Werbeaktionen, Gewinnspielen so lange dies für die Durchführung erforderlich ist und darüber hinaus für einen Zeitraum von 24 Monaten.

Sofern Sie künftigen Werbezusendungen widersprechen, sperren wir Ihre Daten, indem wir Ihren Namen, die Adresse und ggfs. die angegebene E-Mail-Adresse in entsprechenden Listen verwenden, mit denen wir unsere Werbemaßnahmen abgleichen. Nur auf diese Weise ist gewährleistet, dass Sie tatsächlich keine Werbezusendungen mehr erhalten.

**1.8 Welche Rechte haben Sie hinsichtlich Ihrer Daten?**

Bezüglich der Verarbeitung Ihrer Daten steht Ihnen ein Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, auf Widerspruch sowie auf Datenübertragbarkeit zu.

Bezüglich der Verarbeitung Ihrer Daten stehen Ihnen folgende Rechte zu:

* Ein Recht auf Auskunft gegen uns in Bezug auf Ihre Daten (Art. 15 DSGVO)
* Ein Recht auf Berichtigung, sofern Ihre Daten unrichtig sind bzw. auf Vervollständigung, sofern Ihre Daten unvollständig sind (Art. 16 DSGVO),
* Ein Recht auf Löschung, (1) wenn eine Verarbeitung Ihrer Daten zu den genannten Zwecken nicht weiter notwendig ist, (2) wenn die Verarbeitung sich auf eine von Ihnen mittlerweile widerrufene Einwilligung stützt und keine andere Rechtsgrundlage für eine Verarbeitung durch uns vorliegt, (3) wenn Sie Widerspruch gegen eine durch uns durchgeführte Verarbeitung erhoben haben, (4) wenn wir Ihre Daten unrechtmäßig verarbeitet haben, oder (5) wenn eine rechtliche Verpflichtung zur Löschung besteht (sog. „Recht auf Vergessenwerden“, Art. 17 DSGVO),
* Ein Recht auf Einschränkung der Verarbeitung, (1) wenn Sie die Richtigkeit Ihrer Daten bestritten haben für den Zeitraum, den wir zur Prüfung der Richtigkeit benötigen, (2) wenn die Verarbeitung Ihrer Daten unrechtmäßig war und Sie eine Einschränkung der Verarbeitung statt einer Löschung wünschen, (3) wenn eine Speicherung durch uns zu den genannten Zwecken nicht länger erforderlich ist, Sie Ihre Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder (4) wenn Sie Widerspruch gegen durch uns durchgeführte Verarbeitung erhoben haben, die auf sich unsere berechtigten Interessen stützt, solange noch nicht feststeht, ob unsere berechtigten Interessen gegenüber Ihren Rechten überwiegen (Art. 18 DSGVO),
* Ein Recht auf Datenübertragbarkeit im Hinblick auf Ihre Daten, die Sie uns zur Verfügung gestellt haben, wenn die Verarbeitung auf Ihrer Einwilligung oder einem Vertrag mit uns beruht, d. h. Sie können Ihre uns zur Verfügung gestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format an sich oder an Dritte herausverlangen (Art. 20 DSGVO),
* Ein Recht auf Widerspruch gegen die Verarbeitung (Art. 21 DSGVO). Siehe dazu im Einzelnen Ziff. 1.9 dieser Datenschutzhinweise.
* Sofern sich unserer Verarbeitung auf Ihre Einwilligung stützt, ein jederzeitiges Recht auf Widerruf Ihrer Einwilligung, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird (Art. Art. 7 Abs. 3 DSGVO).

Diese Rechte sind teilweise gesetzlich eingeschränkt. Sofern wir diese Rechte daher nicht erfüllen können, werden wir Ihnen dies mitteilen.

**1.9 Widerspruchsrechte gem. Art. 21 DSGVO**

**- Widerspruchsrecht gegen Direktwerbung:**Sie können einer weiteren Verwendung Ihrer Daten zu Werbezwecken jederzeit widersprechen, selbst wenn die Nutzung der Daten auch ohne Ihre Einwilligung gesetzlich zulässig ist. Eine formlose Mitteilung an uns genügt (Kontaktdaten siehe Ziff. 4 unten). Kosten werden dafür von unserer Seite selbstverständlich keine erhoben.  
Folge eines Widerspruchs ist der Stopp der künftigen Verwendung. Dem Widerspruch vorangegangene Nutzungen bleiben unberührt. Hinweise zur Sperrung Ihrer Daten (Einschränkung der Verarbeitung) entnehmen Sie bitte Ziff. 1.8 dieser Datenschutzhinweise.  
In unseren werblichen E-Mails ist jeweils ein Hinweis mit einem Link zur einfachen Ausübung Ihrer Widerspruchsmöglichkeit enthalten.

**- Widerspruchsrecht aus persönlichen Gründen:**Sie haben das Recht aus Gründen, die sich aus Ihrer besonderen Situation ergeben, der Datenverarbeitung durch uns zu widersprechen, soweit sich diese auf unsere berechtigten Interessen stützt. Wir werden dann die Verarbeitung Ihrer Daten einstellen, es sei denn, wir können zwingende schutzwürdige Gründe für die Weiterverarbeitung nachweisen, welche Ihre Rechte überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Weitere Hinweise zu Ihren Rechten können Sie unter Ziff. 4 „Kontakt, Geltendmachung Ihrer Rechte“ entnehmen.

**2. Cookies und ähnliche Technologien von t-online.de**

Neben Cookies nutzen wir auf unserer Website auch weitere Technologien. Im Folgenden bezeichnen wir alle zusammenfassend als „**Cookies**“.

**2.1 Cookies**

Wenn Sie unsere Webseite besuchen, sammeln wir Informationen über Sie, indem wir Cookies einsetzen. Cookies sind kleine Textdateien, die eine Wiedererkennung Ihres Browsers ermöglichen und die an Ihren Computer oder Ihr mobiles Gerät gesendet werden. Wir verwenden Cookies, um Ihnen eine nutzerfreundliche und sichere Webseite anbieten zu können und unsere Dienste an Ihre Bedürfnisse und Interessen anzupassen, z.B., indem wir Ihr Browser-Erlebnis individualisieren oder Ihnen auf Sie zugeschnittene Werbung auf unserer Webseite anzeigen.

Wir verwenden verschiedene Arten von Cookies:

* **Session Cookies**  
  - Session Cookies ermöglichen es, Ihre Aktivitäten auf der Website während Ihrer Browser-Session zu speichern. Diese Cookies werden nach Schließen Ihres Browsers oder nach Schließen der Website gelöscht.
* **Permanente Cookies**  
  - Permanente Cookies werden über eine konkrete Browser-Session hinaus für einen festgelegten Zeitraum gespeichert. Diese Cookies werden auch als „Tracking-Cookies“, „Analyse-Cookies“ oder „Conversion-Cookies“ bezeichnet und helfen uns dabei, Ihren Browser, Ihre Interessen und Ihr Nutzerverhalten zu erkennen und das Angebot entsprechend an Ihre individuellen Bedürfnisse anzupassen. Durch die Verwendung dieser Cookies besteht auch die Möglichkeit, Ihre Nutzung zu optimieren, da registriert wird, wie, wann und wie oft Sie die Dienste nutzen und auf welche Links Sie klicken. Das ermöglicht beispielsweise auf Sie zugeschnittene Trends, Geschichten, Anzeigen und Follower-Vorschläge. Außerdem ermöglichen Tracking-Cookies, dass Sie auf der Website eingeloggt bleiben, ohne Ihre Anmeldedaten erneut eingeben müssen.

**Ihre Rechte / Einstellungsmöglichkeiten:**

Abgesehen von sogenannten unbedingt erforderlichen Cookies verarbeiten wir Cookies nur mit Ihrer Einwilligung, die Sie über den Privacy Manager erteilen und widerrufen können. Unbedingt erforderliche Cookies sind Cookies, die für die Bereitstellung unserer Angebote technisch notwendig sind (z.B. der Cookie, über den unser Privacy Manager funktioniert, und mit dessen Hilfe Ihre dortigen Einstellungen gespeichert werden).  
Natürlich können Sie unsere Angebote auch ohne Cookies nutzen. Browser lassen sich so einstellen, dass Cookies generell abgelehnt werden. Ebenso können Sie bereits gesetzte Cookies in Ihren Browser-Einstellungen löschen. Wenn Sie keine Cookies zulassen, könnte dies jedoch dazu führen, dass Sie die Funktionen unserer Webseite nicht mehr in vollem Umfang nutzen können.

**2.2 Ähnliche Technologie**

**Conversion Tracking**

Wenn Sie über eine Google-Anzeige, eine Affiliate-Anzeige oder eine E-Mail der Telekom auf unsere Webseiten gelangt sind, können mithilfe eines Cookies von Google AdWords, Metalyzer oder Teradata, das nach 30 Tagen seine Gültigkeit verliert, Statistiken über unsere Konversionsrate erstellt werden („Conversion-Cookies“). Das bedeutet, dass wir erfahren, wie viele Nutzer über einen der oben genannten Wege unsere Webseite besuchen und innerhalb von 30 TagWenn Sie über eine Google-Anzeige, eine Affiliate-Anzeige oder eine E-Mail der Telekom auf unsere Webseiten gelangt sind, können mithilfe eines Cookies von Google AdWords, Metalyzer oder Teradata, das nach 30 Tagen seine Gültigkeit verliert, Statistiken über unsere Konversionsrate erstellt werden („Conversion-Cookies“). Das bedeutet, dass wir erfahren, wie viele Nutzer über einen der oben genannten Wege unsere Webseite besuchen und innerhalb von 30 Tagen ein Produkt über unsere Webseiten erwerben. Ein Rückschluss auf Ihre Person ist dabei nicht möglich.en ein Produkt über unsere Webseiten erwerben. Ein Rückschluss auf Ihre Person ist dabei nicht möglich.

**Ihre Rechte / Widerspruch:**

Wenn Sie nicht an dem Tracking-Verfahren teilnehmen möchten, können Sie die Conversion-Cookies deaktivieren, indem Sie in Ihren Browser-Einstellungen festlegen, dass Cookies von der entsprechenden Domain blockiert werden:

Google Adwords: [ads.google.com](https://ads.google.com/)  
Metalyzer: [tracking.mlsat02.de](https://tracking.mlsat02.de/) und [tracking.metalyzer.com](https://tracking.metalyzer.com/optout/)  
Teradata: [email-telekom.de](https://email-telekom.de/)

3. Von uns eingesetzte Technologien

Wir setzen auf unserer Website die in diesem Abschnitt beschriebenen Technologien ein. Die Technologien werden zum Teil von unseren Partnern betrieben, die dabei Daten in unserem Auftrag verarbeiten („Auftragsverarbeitung“).

**3.1 Google-Analytics**

Wir verwenden den Analysedienst Google Analytics der Firma Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google). Die durch den Cookie erzeugten Informationen über Ihre Benutzung der Webseite werden an einen Server von Google in den USA übertragen und dort gespeichert.  
Google wird in unserem Auftrag diese Informationen benutzen, um die Nutzung unserer Webseite auszuwerten, um Reports über Webseiten-aktivitäten zusammenzustellen und um weitere mit der Webseitennutzung und der Internetnutzung verbundene Dienstleistungen uns gegenüber zu erbringen. Aus den verarbeiteten Daten können pseudonyme Nutzungsprofile erstellt werden.  
Wir haben auf unserer Webseite Google Analytics um den Code „anonymizeIP“ erweitert. Dies bedeutet, die IP-Adresse der Nutzer wird innerhalb der EU oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum gekürzt. Nur in Ausnahmefällen wird die volle IP-Adresse an einen Server von Google in den USA übertragen und dort gekürzt. Die im Rahmen von Google Analytics von Ihrem Browser übermittelte IP-Adresse wird nicht mit anderen Daten von Google zusammengeführt.  
Die Gesetze zum Schutz von personenbezogenen Daten können in den USA von dem Schutz innerhalb der EU abweichen und gegebenenfalls nur ein geringeres Schutzniveau gewährleisten. Sollten personenbezogene Daten durch Google Analytics in den USA verarbeitet werden findet dies auf Basis geeigneter Vertraulichkeits- und Sicherheitsmaßnahmen statt, die den Schutz Ihrer Daten sicherstellen.

**Ihre Rechte / Widerspruch:**  
  
Die Speicherung der Cookies können Sie durch eine entsprechende Einstellung in Ihrem Browser verhindern. Sie können darüber hinaus die Erfassung der durch das Cookie erzeugten und auf Ihre Nutzung dieser Website bezogenen Daten an Google sowie die Verarbeitung dieser Daten durch Google verhindern, indem Sie das unter dem folgenden Link verfügbare Browser-Plugin herunterladen und installieren: https://tools.google.com/dlpage/gaoptout?hl=de .  
Die Webanalyse bleibt in diesem Fall solange deaktiviert, wie das Add-On von Google nicht seinerseits deaktiviert bzw. gelöscht wird. Daher löschen Sie bitte das Add-On nicht, solange die Webanalyse nicht gewollt ist. Das Add-On ist pro Browser und Rechner gesetzt. Falls Sie unsere Webseite also mit unterschiedlichen Browsern oder von unterschiedlichen Rechnern aus aufrufen, müssen Sie für jeden Browser bzw. Rechner das Add-On gesondert hinzufügen. Alternativ zum Browser-Add-On, insbesondere bei Browsern auf mobilen Endgeräten, können Sie die Erfassung durch Google Analytics zudem verhindern, indem Sie auf diesen Link klicken: [Google Analytics Tracking beenden](https://www.t-online.de/google-analytics-tracking-beenden/id_81071574/index).  
  
Es wird ein Opt-Out-Cookie gesetzt, das die zukünftige Erfassung Ihrer Daten beim Besuch dieser Website verhindert. Der Opt-Out-Cookie gilt nur in diesem Browser und nur für unsere Website und wird auf Ihrem Gerät abgelegt. Löschen Sie die Cookies in diesem Browser, müssen Sie das Opt-Out-Cookie erneut setzen. Wir nutzen Google Analytics des Weiteren dazu, Daten aus DoubleClick-Cookies und auch AdWords zu statistischen Zwecken auszuwerten. Dies umfasst demografischen Merkmale (z.B. Alter und Geschlecht) sowie Interessen. Diese Daten sind nicht auf eine bestimmte Person zurückzuführen. Sollten Sie dies nicht wünschen, können Sie dies jederzeit über die Anzeigeneinstellungen deaktivieren.

**3.2 Google Analytics Remarketing**

Unsere Websites nutzen die Funktionen von Google Analytics Remarketing in Verbindung mit den geräteübergreifenden Funktionen von Google AdWords und Google DoubleClick. Anbieter ist die Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.  
Diese Funktion ermöglicht es, die mit Google Analytics Remarketing erstellten Werbe-Zielgruppen mit den geräteübergreifenden Funktionen von Google AdWords und Google DoubleClick zu verknüpfen. Auf diese Weise können interessenbezogene, personalisierte Werbebotschaften, die in Abhängigkeit Ihres früheren Nutzungs- und Surfverhaltens auf einem Endgerät (z.B. Handy) an Sie angepasst wurden auch auf einem anderen Ihrer Endgeräte (z.B. Tablet oder PC) angezeigt werden.  
Haben Sie eine entsprechende Einwilligung erteilt, verknüpft Google zu diesem Zweck Ihren Web- und App-Browserverlauf mit Ihrem Google-Konto. Auf diese Weise können auf jedem Endgerät, auf dem Sie sich mit Ihrem Google-Konto anmelden, dieselben personalisierten Werbebotschaften geschaltet werden.  
Zur Unterstützung dieser Funktion erfasst Google Analytics Google-authentifizierte IDs der Nutzer, die vorübergehend mit unseren Google-Analytics-Daten verknüpft werden, um Zielgruppen für die geräteübergreifende Anzeigenwerbung zu definieren und zu erstellen.  
Sie können dem geräteübergreifenden Remarketing/Targeting dauerhaft widersprechen, indem Sie personalisierte Werbung in Ihrem Google-Konto deaktivieren; folgen Sie hierzu diesem Link: https://www.google.com/settings/ads/onweb/  
Die Zusammenfassung der erfassten Daten in Ihrem Google-Konto erfolgt ausschließlich auf Grundlage Ihrer Einwilligung, die Sie bei Google abgeben oder widerrufen können (Art. 6 Abs. 1 lit. a DSGVO). Bei Datenerfassungsvorgängen, die nicht in Ihrem Google-Konto zusammengeführt werden (z.B. weil Sie kein Google-Konto haben oder der Zusammenführung widersprochen haben) beruht die Erfassung der Daten auf Art. 6 Abs. 1 lit. f DSGVO. Das berechtigte Interesse ergibt sich daraus, dass der Websitebetreiber ein Interesse an der anonymisierten Analyse der Websitebesucher zu Werbezwecken hat.  
Weitergehende Informationen und die Datenschutzbestimmungen finden Sie in der Datenschutzerklärung von Google unter: https://policies.google.com/technologies/ads?hl=de

**3.3 Google AdWords und Google Conversion-Tracking**

Diese Website verwendet Google AdWords. AdWords ist ein Online-Werbeprogramm der Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States (“Google”).  
Im Rahmen von Google AdWords nutzen wir das so genannte Conversion-Tracking. Wenn Sie auf eine von Google geschaltete Anzeige klicken wird ein Cookie für das Conversion-Tracking gesetzt. Bei Cookies handelt es sich um kleine Textdateien, die der Internet-Browser auf dem Computer des Nutzers ablegt. Diese Cookies verlieren nach 30 Tagen ihre Gültigkeit und dienen nicht der persönlichen Identifizierung der Nutzer. Besucht der Nutzer bestimmte Seiten dieser Website und das Cookie ist noch nicht abgelaufen, können Google und wir erkennen, dass der Nutzer auf die Anzeige geklickt hat und zu dieser Seite weitergeleitet wurde.  
Jeder Google AdWords-Kunde erhält ein anderes Cookie. Die Cookies können nicht über die Websites von AdWords-Kunden nachverfolgt werden. Die mithilfe des Conversion-Cookies eingeholten Informationen dienen dazu, Conversion-Statistiken für AdWords-Kunden zu erstellen, die sich für Conversion-Tracking entschieden haben. Die Kunden erfahren die Gesamtanzahl der Nutzer, die auf ihre Anzeige geklickt haben und zu einer mit einem Conversion-Tracking-Tag versehenen Seite weitergeleitet wurden. Sie erhalten jedoch keine Informationen, mit denen sich Nutzer persönlich identifizieren lassen. Wenn Sie nicht am Tracking teilnehmen möchten, können Sie dieser Nutzung widersprechen, indem Sie das Cookie des Google Conversion-Trackings über ihren Internet-Browser unter Nutzereinstellungen leicht deaktivieren. Sie werden sodann nicht in die Conversion-Tracking Statistiken aufgenommen.  
Die Speicherung von “Conversion-Cookies” und die Nutzung dieses Tracking-Tools erfolgen auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Der Websitebetreiber hat ein berechtigtes Interesse an der Analyse des Nutzerverhaltens, um sowohl sein Webangebot als auch seine Werbung zu optimieren.  
Mehr Informationen zu Google AdWords und Google Conversion-Tracking finden Sie in den Datenschutzbestimmungen von Google: https://policies.google.com/privacy?hl=de.  
Sie können Ihren Browser so einstellen, dass Sie über das Setzen von Cookies informiert werden und Cookies nur im Einzelfall erlauben, die Annahme von Cookies für bestimmte Fälle oder generell ausschließen sowie das automatische Löschen der Cookies beim Schließen des Browsers aktivieren. Bei der Deaktivierung von Cookies kann die Funktionalität dieser Website eingeschränkt sein.

**3.4 Taboola**

Wir setzen auf unsere Webseite den Service von Taboola ein, der es ermöglicht, nutzerindividuelle Empfehlungen für Inhalte und Anzeigen auf Basis von Surfverhalten und Kundeninteressen auszuspielen, um damit die Nutzerfreundlichkeit unseres Angebots zu verbessern. Die Nutzungsprofile werden unter Verwendung von Pseudonymen erstellt, sie werden nicht mit den Daten über den Träger des Pseudonyms zusammengeführt und lassen keine Rückschlüsse auf persönliche Daten zu. Taboola erhebt mittels Cookies folgende Nutzer-Informationen:  
- Betriebssystem des Nutzers  
- Aufgerufene Webseiten/Inhalte auf unseren Webseiten  
- Referrer/Link, über den der User auf unsere Website gekommen ist  
- Zeitpunkt und Anzahl der Website-Aufrufe  
- Aufrufe von Fehlerseiten  
- Standortinformationen (Stadt und Bundesland)  
- IP-Adressen in gekürzter Form

**Ihre Rechte / Widerspruch**:  
  
Weitere Informationen zu Taboola finden Sie unter https://www.taboola.com/privacy-policy .  
Dort können Sie im Abschnitt „User Choices“ jederzeit das Tracking deaktivieren.  
Nach erfolgtem Opt-Out werden Ihnen keine personalisierten Inhalte/Werbung mehr ausgespielt.

**3.5 Civey**

Wir erheben Online-Umfragen mit der Civey GmbH (im folgenden Civey genannt). Civey hat eine Datenlogik entwickelt, mit der repräsentative Meinungsumfragen erstellt und ausgewertet werden können. Civey ermöglicht seinen Nutzern, sich an repräsentativen Umfragen zu beteiligen und die Ergebnisse direkt einzusehen. Sie haben die Möglichkeit an diesen Online-Umfragen anonym teilzunehmen. In diesem Fall erhebt Civey keine personenbezogenen Daten. Sie können sich jedoch auch bei Civey mit Ihrer E-Mail-Adresse registrieren und als registriertes Civey-Mitglied an den Online-Umfragen teilnehmen. Nutzer, die sich mit einer E-Mail Adresse registrieren, müssen die Nutzungsbedingungen von Civey akzeptieren. Hinsichtlich der Erhebung, Verarbeitung und Nutzung der betreffenden Daten im Falle einer Registrierung gelten die Nutzungsbedingungen und Datenschutzhinweise von Civey. Diese finden Sie hier: www.civey.com/nutzungsbedingungen und www.civey.com/datenschutz  
  
Ein Widerspruch / Opt-Out kann per Mail an datenschutz@civey.com eingereicht werden.

**3.6 Conversario**

Conversario erhebt, verarbeitet und nutzt Ihre personenbezogenen Daten nur unter Einhaltung der einschlägigen Datenschutzbestimmungen und nur soweit es notwendig ist, damit sie unsere Software nutzen können. Darüber hinaus erheben Conversario Zugriffsdaten auf ihren Server sowie Statistikdaten.  
In keinem Fall wird Conversario Ihre personenbezogenen Daten zu Werbe- oder Marketingzwecken oder unbefugt zu anderen Zwecken Dritten übermitteln. Ihre Daten werden nur dann an Dritte weiter geleitet, wenn dies gesetzlich erlaubt ist oder Sie in die Weiterleitung eingewilligt haben.  
Conversario trifft organisatorische, vertragliche und technische Sicherheitsmaßnahmen, um sicher zu stellen, dass die Vorschriften der Datenschutzgesetze eingehalten werden und damit die durch Conversario verwalteten Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen.  
Weitere Informationen dazu finden Sie unter https://www.conversar.io/de/privacy.html .

Link zum Opt-Out: https://tools.google.com/dlpage/gaoptout?hl=de

**3.7 Opinary**

Opinary-Tools werden auf t-online.de eingebunden und ermöglichen Ihnen interaktiv Ihre Meinung abzugeben. Bei der Nutzung eines Opinary-Tools werden keine personenbezogenen Daten erhoben. Die IP-Adressen der anfragenden Rechner werden verkürzt und somit anonymisiert protokolliert. Eine Rückverfolgung ist nicht möglich.  
Cookies: Bei der Nutzung von Opinary-Tools werden Cookies auf Ihrem Browser in dem dafür vorgesehenen Verzeichnis abgelegt. Die Cookies dienen dazu, dass ein und derselbe Nutzer nicht mehrfach an einer Umfrage teilnehmen kann. Über den Cookie wird somit lediglich die Information gespeichert, wer bereits an der Umfrage teilgenommen hat. Über die Cookies werden ausschließlich die verkürze IP-Adresse sowie die anonymisierten Logfile-Datensätze (u.a. Datum und Uhrzeit des Abrufs, Browsertyp und -version) übermittelt. Weitere Informationen zu Opinary: opinary.com/datenschutz/  
  
Link zum Opt-Out: https://compass.pressekompass.net/static/optout.html

**3.8 Heatmap**

Die HeatMap Inc. stellt ein Tool zur Verfügung, womit das Klickverhalten der Nutzer auf t-online.de analysiert werden kann. Dabei werden Daten vom Endgerät, mit dem der Nutzer t-online.de besucht, an HeatMap anonymisiert übertragen. Es wird die Mausbewegung und das Klickverhalten, die Display-Größe des Endgerätes, der Zugriffsort, die Anzahl der Seitenaufrufe und Datum und Uhrzeit übermittelt.  
Weitere Informationen und die Möglichkeit zum Opt-Out finden Sie auf https://heatmap.me/privacy.

**3.9 Seeding Alliance**

Seeding Alliance erfasst anonymisierte Informationen über das Userverhalten, beispielsweise welche Inhalte oder Produkte angesehen wurden, die Native Advertising Kampagnen von Seeding Alliance ausspielen. Dies hilft Seeding Alliance, Native Advertising Kampagnen besser auszusteuern und Ihnen relevantere Werbung anzuzeigen. Alle erfassbaren Informationen werden von Seeding Alliance anonymisiert einer mehrstelligen Identifikationsnummer zugeordnet, die in einem Cookie auf dem Rechner des Users gespeichert wird. So ist es nicht möglich einen Rückschluss auf die Identität zu erhalten. Sofern IP-Adressen erfasst werden, geschieht dies unmittelbar anonymisiert.  
  
Erhobene Daten werden in Rechenzentren innerhalb der EU verarbeitet und verschlüsselt und datenschutzkonform gespeichert. Personenbezogene Daten werden grundsätzlich nicht erhoben.  
  
Weitere Informationen: https://seeding-alliance.de/datenschutz/  
  
Link zum Opt-Out: https://seeding-alliance.de/opt-out/

**3.10 trbo (www.trbo.com/)**

Auf unserer Seite werden durch die trbo GmbH, Römerstrasse 6, 80801 München (http://www.trbo.com/) Daten erhoben und gespeichert, aus denen unter Verwendung von Pseudonymen Nutzungsprofile erstellt werden, um Ihnen personalisierte Kundenvorteile auszuspielen. Zu diesem Zweck können Cookies eingesetzt werden, die die Wiedererkennung eines Internet Browsers ermöglichen. Diese Nutzungsprofile dienen der Analyse des Besucherverhaltens und werden zur Verbesserung und bedarfsgerechten Gestaltung unseres Angebots ausgewertet. Die pseudonymisierten Nutzungsprofile werden ohne eine gesondert zu erteilende, ausdrückliche Einwilligung des Betroffenen nicht mit personenbezogenen Daten über den Träger des Pseudonyms zusammengeführt. Sie können dies jederzeit widersprechen durch Klick auf die folgenden Links: trbo aktivieren und trbo deaktivieren.  
  
Link Datenschutzhinweise: https://www.trbo.com/datenschutz/  
  
Link zum Opt-Out: https://track2.trbo.com/optout.php?redirect=https%3A%2F%2Fwww.stroeerdigitalpublishing.de%2Fdatenschutz%2F

**3.11 Criteo (https://www.criteo.com/de)**

Auf unserer Seite werden durch die Criteo SA, 32 Rue Blanche, 75009, Paris (https://www.criteo.com/de) Daten erhoben und gespeichert für den Zweck der personalisierten Werbung, speziell des Retargetings. Das ermöglicht das Anzeigen von Werbebannern, welche auf die Interessen der User zugeschnitten sind. Retargeting-Technologien verwenden Cookies oder Werbe-IDs, um Werbung basierend auf dem bisherigen Surfverhalten auf Partner-Webseiten und -Apps bereitzustellen. Weitere Informationen zu verwendeten Tracking-Technologien der Criteo-Partner finden Sie in den Criteo-Datenschutzbestimmungen. Sie können dort der Erhebung bzw. Auswertung Ihrer Daten durch dieses Tool widersprechen, indem Sie das unter dem folgenden Link verfügbare Opt-Out Cookie herunterladen bzw. setzen und speichern.

Link Datenschutzhinweise: https://www.criteo.com/privacy/

Link zum Opt-Out: https://www.criteo.com/de/privacy/

**3.12 SpeedCurve (https://speedcurve.com/)**

Unsere Webseite nutzt das Tool LUX (Live User Xperience) der SpeedCurve Limited (36 Valley Road, Titirangi, Auckland 0604, Neuseeland; „SpeedCurve“). Dieses Tool sammelt Informationen zum Browserverhalten, im speziellen Seitendetails, Seitendesign, Interaktionsmetriken und nutzt dazu die Browser NavigationTiming-, UserTiming-, NetworkInformation-, und PaintTiming-API.

LUX erhebt keine personenbezogenen Daten wie IP-Adressen, Cookies oder LocalStorage.

Die durch LUX erzeugten Informationen werden in unserem Auftrag an einen Server von SpeedCurve in Neuseeland übertragen und dort für drei Monate gespeichert. Diese Informationen nutzen wir, um die Nutzung der Webseite auszuwerten und unsere Dienste und Angebote für Sie zu optimieren. Die EU-Kommission hat die Angemessenheit des Datenschutzniveaus in Neuseeland mit Beschluss vom 19.12.2012 (Az. C(2012) 9557) festgestellt. Den Beschluss der EU-Kommission können Sie [hier](https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013D0065&from=DE) einsehen. Die Datenschutzhinweise von SpeedCurve finden Sie [hier](https://speedcurve.com/terms/). Die Verarbeitung erfolgt auf der Rechtsgrundlage des Art. 6 Abs. 1 lit. f DSGVO.

**4. Technologien von eigenverantwortlichen Dritten**

Des Weiteren finden sich auf unserer Website Technologien, die von eigenverantwortlichen Dritten betrieben werden.

**4.1 Reichweitenmessung / Webanalyse**

* **(1) Messverfahren der INFOnline GmbH**

Unsere Webseite nutzt das Messverfahren („SZMnG“) der INFOnline GmbH ( [https://www.INFOnline.de](https://www.infonline.de/)) zur Ermittlung statistischer Kennwerte über die Nutzung unserer Angebote. Ziel der Nutzungsmessung ist es, die Anzahl der Besuche auf unserer Website, die Anzahl der Websitebesucher und deren Surfverhalten statistisch – auf Basis eines einheitlichen Standardverfahrens - zu bestimmen und somit marktweit vergleichbare Werte zu erhalten.

Für alle Digital-Angebote, die Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW – [https://www.ivw.eu](https://www.ivw.eu/) ) sind oder an den Studien der Arbeitsgemeinschaft Online-Forschung e.V. (AGOF - [https://www.agof.de](https://www.agof.de/) ) teilnehmen, werden die Nutzungsstatistiken regelmäßig von der AGOF und der Arbeitsgemeinschaft Media-Analyse e.V. (agma - [https://www.agma-mmc.de](https://www.agma-mmc.de/) ) zu Reichweiten weiter verarbeitet und mit dem Leistungswert „Unique User“ veröffentlicht sowie von der IVW mit den Leistungswerten „Page Impression“ und „Visits“. Diese Reichweiten und Statistiken können auf den jeweiligen Webseiten eingesehen werden.

**- Zweck der Verarbeitung der Daten** ist die Erstellung von Statistiken und die Bildung von Nutzerkategorien. Die Statistiken dienen dazu, die Nutzung unseres Angebots nachvollziehen und belegen zu können. Die Nutzerkategorien bilden die Grundlage für eine interessengerechte Ausrichtung von Werbemitteln bzw. Werbemaßnahmen. Zur Vermarktung dieser Webseite ist eine Nutzungsmessung, welche eine Vergleichbarkeit zu anderen Marktteilnehmern gewährleistet, unerlässlich. Unser berechtigtes Interesse ergibt sich aus der wirtschaftlichen Verwertbarkeit der sich aus den Statistiken und Nutzerkategorien ergebenden Erkenntnisse und dem Marktwert unserer Webseite - auch in direktem Vergleich mit Webseiten Dritter - der sich anhand der Statistiken ermitteln lässt. Darüber hinaus haben wir ein berechtigtes Interesse daran, die pseudonymisierten Daten der INFOnline, der AGOF und der IVW zum Zwecke der Marktforschung (AGOF, agma) und für statistische Zwecke (INFOnline, IVW) zur Verfügung zu stellen. Weiterhin haben wir ein berechtigtes Interesse daran, die pseudonymisierten Daten der INFOnline zur Weiterentwicklung und Bereitstellung interessengerechter Werbemittel zur Verfügung zu stellen.

**- Art der Daten**

Die INFOnline GmbH erhebt die folgenden Daten:

**IP-Adresse:** Im Internet benötigt jedes Gerät zur Übertragung von Daten eine eindeutige Adresse, die sogenannte IP-Adresse. Die zumindest kurzzeitige Speicherung der IP-Adresse ist aufgrund der Funktionsweise des Internets technisch erforderlich. Die IP-Adressen werden vor jeglicher Verarbeitung um 1 Byte gekürzt und nur anonymisiert weiterverarbeitet. Es erfolgt keine Speicherung oder weitere Verarbeitung der ungekürzten IP-Adressen.

**Einen zufällig erzeugten Client-Identifier:** Die Reichweitenverarbeitung verwendet zur Wiedererkennung von Computersystemen alternativ entweder ein Cookie mit der Kennung „ioam.de", ein „Local Storage Object“ oder eine Signatur, die aus verschiedenen automatisch übertragenen Informationen Ihres Browsers erstellt wird. Diese Kennung ist für einen Browser eindeutig, solange das Cookie oder Local Storage Object nicht gelöscht wird. Eine Messung der Daten und anschließende Zuordnung zu dem jeweiligen Client-Identifier ist daher auch dann möglich, wenn Sie andere Webseiten aufrufen, die ebenfalls das Messverfahren („SZMnG“) der INFOnline GmbH nutzen. Die Gültigkeit des Cookies ist auf maximal 1 Jahr beschränkt.

**- Nutzung der Daten**

Das Messverfahren der INFOnline GmbH, welches auf dieser Webseite eingesetzt wird, ermittelt Nutzungsdaten. Dies geschieht, um die Leistungswerte Page Impressions, Visits und Clients zu erheben und weitere Kennzahlen daraus zu bilden (z.B. qualifizierte Clients). Darüber hinaus werden die gemessenen Daten wie folgt genutzt:  
  
Eine sogenannte Geolokalisierung, also die Zuordnung eines Webseitenaufrufs zum Ort des Aufrufs, erfolgt ausschließlich auf der Grundlage der anonymisierten IP-Adresse und nur bis zur geographischen Ebene der Bundesländer / Regionen. Aus den so gewonnenen geographischen Informationen kann in keinem Fall ein Rückschluss auf den konkreten Aufenthaltsort eines Nutzers gezogen werden.  
  
Die Nutzungsdaten eines technischen Clients (bspw. eines Browsers auf einem Gerät) werden webseitenübergreifend zusammengeführt und in einer Datenbank gespeichert. Diese Informationen werden zur technischen Abschätzung der Sozioinformation Alter und Geschlecht verwendet und an die Dienstleister der AGOF zur weiteren Reichweitenverarbeitung übergeben. Im Rahmen der AGOF-Studie werden auf Basis einer zufälligen Stichprobe Soziomerkmale technisch abgeschätzt, welche sich den folgenden Kategorien zuordnen lassen: Alter, Geschlecht, Nationalität, Berufliche Tätigkeit, Familienstand, Allgemeine Angaben zum Haushalt, Haushalts-Einkommen, Wohnort, Internetnutzung, Online-Interessen, Nutzungsort, Nutzertyp.

**- Speicherdauer der Daten**

Die vollständige IP-Adresse wird von der INFOnline GmbH nicht gespeichert. Die gekürzte IP-Adresse wird maximal 60 Tage gespeichert. Die Nutzungsdaten in Verbindung mit dem eindeutigen Identifier werden maximal 6 Monate gespeichert.

**- Weitergabe der Daten**

Die IP-Adresse wie auch die gekürzte IP-Adresse werden nicht weitergegeben. Für die Erstellung der AGOF-Studie werden Daten mit Client-Identifiern an die folgenden Dienstleister der AGOF weitergegeben:

Kantar Deutschland GmbH (<https://www.kantardeutschland.de/>)  
Ankordata GmbH & Co. KG ( <https://www.ankordata.de/homepage/>)  
Interrogare GmbH ( <https://www.interrogare.de/>)

**Ihre Rechte / Widerspruch:**

Wenn Sie an der Messung nicht teilnehmen möchten, können Sie unter folgendem Link widersprechen: [https://optout.ioam.de](https://optout.ioam.de/)

Weitere Informationen zum Datenschutz im Messverfahren finden Sie auf der Webseite der INFOnline GmbH ( [https://www.infonline.de](https://www.infonline.de/)), die das Messverfahren betreibt, der Datenschutzwebseite der AGOF ([https://www.agof.de/datenschutz](https://www.agof.de/datenschutz/) ) und der Datenschutzwebseite der IVW ( [https://www.ivw.eu](https://www.ivw.eu/)).

* **(2) Webseiten-Analyse mit Webtrekk und Tealium**

Wir verwenden die Dienste der Firma Webtrekk GmbH, um statistische Daten über die Nutzung von t-online.de zu erheben und unser Angebot entsprechend zu optimieren. Die Webtrekk GmbH ist für Datenschutz, im Bereich Web Controlling Software, vom TÜV Saarland zertifiziert. Teil der Zertifizierung ist ein Audit bei Webtrekk vor Ort in Berlin und im Hosting-Standort, in dem die Erfassung und Verarbeitung von Tracking-Daten auf Datenschutzkonformität und Datensicherheit hin geprüft wurden.  
Im Rahmen Ihres Besuchs der Anwendung werden für unser Webcontrolling einige Informationen erhoben und ausgewertet, die Ihr Browser übermittelt. Die Erhebung erfolgt durch einen Pixel, der auf jeder Seite eingebunden ist und durch Cookies.  
  
Folgende Daten werden erhoben:

- Request (Dateiname der angeforderten Datei)  
- Browsertyp/-version (Bsp.: Internet Explorer 6.0)  
- Browsersprache (Bsp.: Deutsch)  
- verwendetes Betriebssystem (Bsp.: Windows XP)  
- innere Auflösung des Browserfensters  
- Bildschirmauflösung  
- Javascriptaktivierung  
- Java An / Aus  
- Cookies An / Aus  
- Farbtiefe  
- Referrer URL (die zuvor besuchte Seite) IP Adresse – wird umgehend anonymisiert und nach Verarbeitung wieder gelöscht  
- Uhrzeit des Zugriffs  
- Klicks  
- Formularinhalte (bei Freitextfeldern, z.B. Name und Passwort, wird nur „ausgefüllt“ oder „nicht ausgefüllt“ übertragen)  
- IP-Adresse – wird ausschließlich in gekürzter, anonymisierter Form gespeichert, nur zur Sessionerkennung, Geolokalisierung (bis auf Stadt-Ebene) und für die Abwehr von Attacken verwendet und direkt nach ihrer Verwendung wieder gelöscht.  
  
**Ihre Rechte / Widerspruch:**  
  
In Ihren Browsereinstellungen können Sie festlegen, ob Cookies gesetzt werden dürfen oder nicht. Wenn Sie spezifisch für t-online.de nicht getrackt werden möchten, können Sie dem Tracking widersprechen. Zur Vervollständigung des Widerspruchs klicken Sie bitte auf den folgenden Link:

[https://www.webtrekk.com/index/datenschutzerklaerung/opt-out.html](https://www.webtrekk.com/opt-out-webtrekk/)

Durch Bestätigung des Links wird ein Cookie mit dem Namen „webtrekkOptOut“ von der Domain Webtrekk.net gesetzt. Dieser Widerspruch gilt so lange, wie Sie das Cookie nicht löschen, maximal jedoch für die Lebensdauer des Cookies von 60 Monaten. Das Cookie ist für die genannte Domain, pro Browser und Rechner gesetzt. Falls Sie daher zum Beispiel unsere Webseite von zu Hause und der Arbeit oder mit unterschiedlichen Browsern besuchen, müssten Sie von jedem Rechner und Browser das Cookie gesondert setzen.

Weitere Informationen finden Sie auf der Website der Webtrekk GmbH: Hannoversche Str. 19, 10115 Berlin: <https://www.webtrekk.com/>

* **(3) Tag-Management mit Tealium**

Tealium IQ ist ein Tag-Management-System mit dem Messpixel von Drittanbietern auf den Seiten der Subdomain https://tarife-und-produkte.t-online.de/ geladen werden (bspw. das Webtrekk Messpixel). Zur Optimierung des Ladens der Messpixel erfasst Tealium über ein Cookie einige nicht personenbezogene Daten. Dieses Cookie verliert nach 12 Monaten seine Gültigkeit. Folgende Informationen werden in dem Tealium Cookie gespeichert:

- Zeitstempel des Webseitenbesuchs  
- ID für den Seitenaufruf  
- ID für den Besucher  
- ID für die Session

**Ihre Rechte / Widerspruch:**

Möchten Sie den Tealium Cookies widersprechen, können Sie diese deaktivieren. Legen Sie in Ihren Browser-Einstellungen fest, dass Cookies von der Domain „tealium.hs.llnwd.net“ oder „tags-eu.tiqcdn.com“ blockiert werden sollen.

**4.2 Werbung / Individualisierung**

**(1) Nutzungsbasierte Werbung – Online Behavorial Advertising (OBA)**

Wenn Sie diese Internetseiten besuchen, werden im Rahmen der gemeinsamen Datenverarbeitung mittels anonymer Benutzernummern durch die in der Consent Management Plattform hinterlegten Vendoren und dem Vermarkter Ströer Digital Media (https://www.stroeer.de/digitale-werbung/werbemedien/targeting-data/datenschutz.html) in einem Cookie Interessen (z.B. geklickte Werbebanner, besuchte Unterseiten, anonymisierte Fragebögen etc.) von Ihnen festgehalten. Diese Daten werden zum Zweck der Einblendung von Inhalten und Werbung passend zu Ihren Interessen verwendet. In keinem Fall werden dabei Daten wie Name, Anschrift, E-Mail-Adresse oder IP-Adresse in den Cookies gespeichert.  
  
Die Auslieferung nutzungsbasierter Online Werbung wird vom digitalen Werbevermarkter [Ströer Digital](https://www.stroeer.de/digitale-werbung.html) betrieben.

**(2) Empfehlungs- und Personalisierungs-System von Taboola Europe Ltd.**

Wir setzen auf unsere Webseite den Service von Taboola ein, der es ermöglicht, nutzerindividuelle Empfehlungen für Inhalte und Anzeigen auf Basis von Surfverhalten und Kundeninteressen auszuspielen, um damit die Nutzerfreundlichkeit unseres Angebots zu verbessern. Die Nutzungsprofile werden unter Verwendung von Pseudonymen erstellt, sie werden nicht mit den Daten über den Träger des Pseudonyms zusammengeführt und lassen keine Rückschlüsse auf persönliche Daten zu. Taboola erhebt mittels Cookies folgende Nutzer-Informationen:

- Betriebssystem des Nutzers  
- Aufgerufene Webseiten/Inhalte auf unseren Webseiten  
- Referrer/Link, über den der User auf unsere Website gekommen ist  
- Zeitpunkt und Anzahl der Website-Aufrufe  
- Aufrufe von Fehlerseiten  
- Standortinformationen (Stadt und Bundesland)  
- IP-Adressen in gekürzter Form

**Ihre Rechte / Widerspruch:**

Weitere Informationen zu Taboola finden Sie unter [https://www.taboola.com/privacy-policy](https://policies.taboola.com/en/privacy-policy/) .  
Dort können Sie im Abschnitt „User Choices“ jederzeit das Tracking deaktivieren.  
Nach erfolgtem OptOut werden Ihnen keine personalisierten Inhalte/Werbung mehr ausgespielt.

**(3) Folgende Tools sind für die Datenerhebung zur Auslieferung von nutzungsbasierter Online-Werbung zuständig:**

**- Sizmek (**[**https://www.sizmek.com**](https://www.sizmek.com/)**)**  
Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Sizmek ist die Sizmek Inc., 500 West 5th Street, Suite 900, Austin, TX 78701, United States. Sizmek setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.sizmek.com/privacy-policy/>

Link zum Opt-Out: <https://www.sizmek.com/privacy-policy/optedout/#options>  
  
**- Flashtalking (**[**https://www.flashtalking.com**](https://www.flashtalking.com/)**)**  
Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Flashtalking ist die Flashtalking Inc., 142 West 36th Street, 10th Floor, New York, NY 10018, United States. Flashtalking setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise:<https://www.flashtalking.com/privacypolicy/>

Link zum Opt-Out: <https://www.flashtalking.com/privacypolicy/>  
  
**- TabMo (**[**https://tabmo.io/**](https://hawk.tabmo.io/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von TabMo ist die TabMo, SAS 2, rue clichy, Paris, 75009, France. TabMo setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: [https://tabmo.io/](https://hawk.tabmo.io/)  
  
**- Splicky (**[**https://www.splicky.com/de**](https://www.splicky.com/de)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Splicky ist die Goldbach Digital Services AG, Seestrasse 353, 8038 Zürich Wollishofen, Schweiz. Splicky setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.splicky.com/de/web/privacy>

Link zum Opt-Out: Nutzer können den Erhalt von Cookies mit einem Klick auf Jaduda unter Präferenzmanagement hier deaktivieren: www.youronlinechoices.eu  
  
**- MediaMath (**[**https://www.mediamath.com/de/**](https://www.mediamath.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von MediaMath ist die MediaMath Inc., 4 World Trade Center, 150 Greenwich Street, 45th Floor, New York, NY 10007, United States. MediaMath setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.mediamath.com/de/datenschutzrichtlinie/>

Link zum Opt-Out: <https://www.mediamath.com/de/ad-choices-opt-out/>  
  
**- IntelliAd (**[**https://www.intelliad.de**](https://www.intelliad.de/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von IntelliAd ist die intelliAd Media GmbH, Sendlinger Str. 7, 80331 München, Deutschland. IntelliAd setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.intelliad.de/datenschutzerklaerung/>

Link zum Opt-Out: <https://www.intelliad.de/opt-out-manager/>  
  
**- Visual IQ (**[**https://www.refinedlabs.com/**](https://www.refinedlabs.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Visual IQ ist die Refined Labs GmbH – A Nielsen Company, Theresienstraße 4-6, 80333 München, Deutschland. Visual IQ setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.refinedlabs.com/datenschutz-rfa>

Link zum Opt-Out: <https://www.refinedlabs.com/datenschutz-rfa>  
  
**- Exactag (**[**https://www.exactag.com/**](https://www.exactag.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Exactag ist die Exactag GmbH, Philosophenweg 17, 47051 Duisburg, Deutschland. Exactag setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.exactag.com/datenschutz/>

Link zum Opt-Out: <https://m.exactag.com/optout.aspx?url=https://www.exactag.com/bestaetigung/>  
  
**- Econda (**[**https://www.econda.de/**](https://www.econda.de/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Econda ist die econda GmbH, Zimmerstr. 6, 76137 Karlsruhe, Deutschland. Econda setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.econda.de/datenschutzhinweise/>

Link zum Opt-Out: <https://www.econda.de/datenschutzhinweise/>  
  
**- Webtrekk (**[**https://www.webtrekk.com/de**](https://www.webtrekk.com/de)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Webtrekk ist die Webtrekk GmbH, Robert-Koch-Platz 4, 10115 Berlin, Deutschland. Webtrekk setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.webtrekk.com/de/legal/opt-out-webtrekk/>

Link zum Opt-Out: <http://optout.webtrekk.net/?r=https://www.webtrekk.com/de/legal/opt-out-webtrekk/abmeldung-vom-tracking/>  
  
**- DoubleVerify (**[**https://www.doubleverify.com/**](https://www.doubleverify.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von DoubleVerify ist die DoubleVerify, Inc., 233 Spring Street, 4th Floor, New York, NY 10013. DoubleVerify setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.doubleverify.com/privacy/>  
  
Link zum Opt-Out: <https://www.doubleverify.com/opt-out/>

**- Moat (**[**https://moat.com/**](https://moat.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Moat ist die Moat Inc., 228 Park Ave South #17953, New York NY 10003, United States. Moat setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://moat.com/privacy>

Link zum Opt-Out: <https://moat.com/privacy#your_choice>  
  
**- Amazon (**[**https://www.aps.amazon.com**](https://aps.amazon.com/aps/index.html)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Amazon publisher services ist die Amazon publisher services, 410 Terry Ave. North, Seattle, WA 98109-5210, Washington, United States. Amazon publisher services setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.amazon.de/gp/help/customer/display.html/ref=dra_oo?ie=UTF8&nodeId=3312401>

Link zum Opt-Out: <https://www.amazon.de/adprefs>  
  
**- ONE (AOL)/Oath**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von ONE ist die Oath (EMEA) Limited, 5-7 Point Square, North Wall Quay, Dublin 1, Ireland. ONE setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://policies.oath.com/ie/de/oath/privacy/index.html>

Link zum Opt-Out: http://optout3.privacy.aol.com/Adapter.aspx  
  
**- Audience Network by Facebook (**[**https://de-de.facebook.com/business/**](https://de-de.facebook.com/business/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Audience Network ist die Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Irland. Audience Network setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://de-de.facebook.com/ads/manage/audience_network/publisher_tos/>

Link zum Opt-Out: [http://www.facebook.com/ads/edaa/optout?token=AckIfuiC\_1c4-SJT](https://www.facebook.com/ads/edaa/optout?token=AckIfuiC_1c4-SJT)  
  
**- bRealTime (**[**https://emxdigital.com**](https://emxdigital.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von bRealTime ist die EMX Digital LLC, 222 North LaSalle Street, Suite 1650, Chicago, IL 60601, USA. bRealTime setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://emxdigital.com/privacy/>

Link zum Opt-Out: [https://optout.aboutads.info/?c=2#!/](https://optout.aboutads.info/?lang=EN&c=2#!%2F)  
  
**- Conversant (**[**https://www.conversantmedia.com**](https://www.conversantmedia.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Conversant ist die Conversant Europe Limited, 1st Floor, 40 Dukes Place, London, EC3A 7NH. Conversant setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.conversantmedia.com/legal/privacy>

Link zum Opt-Out: https://optout.conversantmedia.com/  
  
**- IndexExchange (**[**http://de.indexexchange.com**](https://de.indexexchange.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von IndexExchange ist die Index Exchange Inc., 74 Wingold Avenue, Toronto, ON M6B 1P5, Canada. IndexExchange setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://de.indexexchange.com/datenschutzerklarung/>

Link zum Opt-Out: [https://optout.networkadvertising.org/#!/](https://optout.networkadvertising.org/?c=1#!%2F)  
  
**- OpenX (**[**https://www.openx.com/de\_de/**](https://www.openx.com/de_de/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von OpenX ist die OpenX Limited, 1-3 Maple Place, London, W1T 4BB, United Kingdom. OpenX setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.openx.com/legal/>

Link zum Opt-Out: <https://u.openx.net/privacy/edaa/optout>  
  
**- PubMatic (**[**https://pubmatic.com**](https://pubmatic.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von PubMatic ist die PubMatic Inc., 305 Main Street, First Floor, Redwood City, CA 9406, USA. PubMatic setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://pubmatic.com/legal/privacy-policy/>

Link zum Opt-Out: <https://pubmatic.com/legal/opt-out/>  
  
**- PulsePoint (**[**https://www.pulsepoint.com**](https://pulsepoint.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von PulsePoint ist die PulsePoint Inc., 360 Madison Avenue, 14th Floor, New York, NY 10017, United States. PulsePoint setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: [https://www.pulsepoint.com/privacy-policy](https://pulsepoint.com/legal/platform-privacy-policy)

Link zum Opt-Out: <https://optout.networkadvertising.org/?c=1#!%2F>  
  
**- Rubicon (**[**http://rubiconproject.com**](https://rubiconproject.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Rubicon ist die The Rubicon Project Ltd., Walmar House, 5th Floor, 296 Regent St., London, W1B 3HR, United Kingdom. Rubicon setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://rubiconproject.com/privacy/>

Link zum Opt-Out: <https://rubiconproject.com/privacy/consumer-online-profile-and-opt-out/>  
  
**- SmartAdServer (**[**https://smartadserver.com**](https://smartadserver.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von SmartAdServer ist die SmartAdServer GmbH, Mehringdamm 33, 10961 Berlin, Deutschland. SmartAdServer setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://smartadserver.com/end-user-privacy-policy/>

Link zum Opt-Out: <http://www.smartadserver.com/diffx/gdprOptoutAll>  
  
**- Sovrn (**[**https://www.sovrn.com**](https://www.sovrn.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Sovrn ist die Sovrn Inc., 5541 Central Ave. #100, Boulder, CO 80301, United States. Sovrn setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.sovrn.com/privacy-policy/>

Link zum Opt-Out: <https://info.evidon.com/pub_info/15620?v=1&nt=0&nw=false>  
  
**- Reachnet (**[**https://www.reachnet.de**](https://www.reachnet.de/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Reachnet ist die Reachnet DE Ltd., Grindelallee 41, 20146 Hamburg, Deutschland. Reachnet setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.reachnet.de/unternehmen/datenschutz.html>

Link zum Opt-Out: <https://adfarm1.adition.com/opt?m=optout&n=73>  
  
**- Primis (**[**https://www.primis.tech/**](https://www.primis.tech/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Primis ist die Primis Inc., 11475 Great Oaks Way, Suite 320, Alpharetta, GA 30022, United States. Primis setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.primis.tech/privacy-policy/>

Link zum Opt-Out: <http://optout.networkadvertising.org/?c=1>  
  
**- Smaato (**[**https://www.smaato.com**](https://www.smaato.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Smaato ist die Smaato Ad Services, Valentinskamp 70, Emporio, 20355 Hamburg, Deutschland. Smaato setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.smaato.com/privacy/>

Link zum Opt-Out: https://www.smaato.com/privacy/  
  
**- MoPub (**[**https://www.mopub.com**](https://www.mopub.com/en)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von MoPub ist die MoPub Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, United States. MoPub setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: [https://www.mopub.com/legal/privacy/](https://www.mopub.com/en/legal/privacy)

Link zum Opt-Out: https://www.mopub.com/legal/privacy/  
  
**- inmobi (**[**https://www.inmobi.com**](https://www.inmobi.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von inmobi ist die Inmobi Pte Ltd., Embassy Tech Square, Kadubeesanahalli Village Outer Ring Roard, Varthur Hobli, Bangalore 560103, India. inmobi setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.inmobi.com/privacy-policy/>

Link zum Opt-Out: <https://www.inmobi.com/page/opt-out/>  
  
**- Advanced Store (**[**https://www.advanced-store.com/de/**](https://www.advanced-store.com/de/)**)**

Advanced Store wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Advanced Store ist die advanced store GmbH, Alte Jakobstraße 79 / 80, 10179 Berlin, Deutschland. Advanced Store setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.advanced-store.com/de/datenschutz/>

Link zum Opt-Out: <https://www.ad4mat.com/de/adchoices/>  
  
**- Factor Eleven (**[**https://www.factor-eleven.de/**](https://www.factor-eleven.de/)**)**

Factor Eleven wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Factor Eleven ist die Factor Eleven GmbH, Siemensstraße 3, Betriebsstätte Fernwald, 35463 Fernwald - Annerod, Deutschland. Factor Eleven setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.factor-eleven.de/datenschutz/>  
  
**- Ligatus (**[**https://www.ligatus.com/de**](https://www.outbrain.com/ligatus/de/)**)**

Ligatus wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Ligatus ist die Ligatus GmbH, Christophstraße 19, 50670 Köln, Deutschland. Ligatus setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: [https://www.ligatus.com/de/privacy-policy](https://www.outbrain.com/ligatus/de/)

Link zum Opt-Out: [https://www.ligatus.com/de/privacy-policy](https://www.outbrain.com/ligatus/de/)  
  
**- mediasports (http://www.mediasports.de)**

mediasports wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von mediasports ist die mediasports Digital GmbH, Kehrwieder 8-10, 2. OG, c/o Ströer Digital Media GmbH, D-20457 Hamburg, Deutschland. mediasports setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: http://www.mediasports.de/impressum

Link zum Opt-Out: [https://optout.ioam.de](https://optout.ioam.de/)  
  
**- M,P,NEWMEDIA (**[**https://www.mp-newmedia.com**](https://www.mp-newmedia.com/)**)**

M,P,NEWMEDIA wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH.  
Anbieter von M,P,NEWMEDIA ist die M,P,NEWMEDIA, GmbH, Hindenburgstraße 45, 71638 Ludwigsburg, Deutschland.  
M,P,NEWMEDIA setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.mp-newmedia.com/datenschutz>

Link zum Opt-Out: <https://www1.mpnrs.com/deliver2/optout/generaloptout?extended=true&remove=false&action=do>  
  
**- Performance Advertising (**[**https://www.performance-advertising.de**](https://www.performance-advertising.de/)**)**

Performance Advertising wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Performance Advertising ist die Performance Advertising GmbH, Gorch-Fock-Wall 1a, 20354 Hamburg, Deutschland. Performance Advertising setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.performance-advertising.de/datenschutz/>

Link zum Opt-Out: <https://www.performance-advertising.de/opt-out/>  
  
**- Advanced Store (**[**https://www.advanced-store.com/de/**](https://www.advanced-store.com/de/)**)**

Advanced Store wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Advanced Store ist die advanced store GmbH, Alte Jakobstraße 79 / 80, 10179 Berlin, Deutschland. Advanced Store setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.advanced-store.com/de/datenschutz/>

Link zum Opt-Out: <https://www.ad4mat.com/de/adchoices/>  
  
**- Plista (**[**https://www.plista.com/de**](https://www.plista.com/de)**)**

Plista wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Plista ist die plista GmbH, Torstraße 33-35, D-10119 Berlin, Deutschland. Plista setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.plista.com/de/ueber/privacy>

Link zum Opt-Out: [https://www.plista.com/about/opt-out/](https://www.plista.com/about/opt-out)  
  
**- Unruly (**[**https://unruly.co/**](https://unruly.co/)**)**

Unruly wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Unruly ist die Unruly Media GmbH, Großer Burstah 36-38, 20457 Hamburg, Deutschland. Unruly setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: [https://unruly.co/privacy/](https://unruly.co/legal/privacy/)

Link zum Opt-Out: <https://video.unrulymedia.com/rtbprivacypolicy/index.html>  
  
**- Just Premium (**[**https://justpremium.com**](https://justpremium.com/)**)**

Just Premium wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Just Premium ist die JustPremium B.V., Constellation CL, Stationsplein Noord-Oost 410, Schiphol, Niederlande. Just Premium setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://justpremium.com/terms-conditions/?section=privacy_policy>

Link Zum Opt-Out: <https://jpx.ads.justpremium.com/opt-out>

**- Taboola (**[**https://www.taboola.com/de**](https://www.taboola.com/de/)**)**

Taboola wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Taboola ist die Taboola, Inc., 1115 Broadway, 7th Floor, New York, NY 10010, USA. Taboola setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://policies.taboola.com/en/privacy-policy/>

Link zum Opt-Out: [https://www.taboola.com/privacy-policy#optout](https://policies.taboola.com/en/privacy-policy/#optout)  
  
**- Xaxis (**[**https://www.xaxis.com**](https://www.xaxis.com/)**)**

Xaxis wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Xaxis ist die Xaxis, LLC., 140 East 45 th St, 12th Floor, New York, NY 10017, United States. Xaxis setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: [https://www.xaxis.com/privacy-policy/](https://www.xaxis.com/privacy-notice/)

Link zum Opt-Out: [https://www.xaxis.com/opt-out/](https://www.xaxis.com/privacy-notice/)  
  
**- ComScore (**[**https://www.comscore.com/ger/**](https://www.comscore.com/ger/)**)**

ComScore wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von ComScore ist die comScore Inc., 11950 Democracy Drive, Suite 600, Reston, VA 20190, United States. ComScore setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.comscore.com/ger/Ueber-Uns/Datenschutzerklaerung>

Link zum Opt-Out: <https://www.comscore.com/ger/Ueber-Uns/Datenschutzerklaerung>  
  
**- Nielsen Digital Ad Ratings (**[**https://www.nielsen.com/de/de/**](https://www.nielsen.com/de/de/)**)**

Nielsen Digital Ad Ratings wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Nielsen Digital Ad Ratings ist die The Nielsen Company (Germany) GmbH, Insterburger Str. 16, 60487 Frankfurt am Main, Deutschland. Nielsen Digital Ad Ratings setzt Analyse-Cookies ein, um das Nutzungsverhalten von Nutzern aufzeichnen und in statistischer Form auswerten zu können.

Link Datenschutzhinweise: <https://www.nielsen.com/de/de/legal/privacy-statement/>

Link zum Opt-Out: <https://server-us.imrworldwide.com/cgi-bin/o?oo=total&tu=http://www.nielsen-online.com/privacy/cookie-policy.html>  
  
**- Forensiq (**[**https://impact.com/protect-monitor/**](https://impact.com/protect-monitor/)**)**

Forensiq wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Nielsen ist die Forensiq Ltd., 50 Eastcastle Street, 3rd Floor, Suite 350, London, W1W 8EA, United Kingdom. Forensiq setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://impact.com/privacy-policy/>  
  
**- Otto Group Media (**[**https://ottogroup.media/**](https://ottogroup.media/)**)**

Otto Group Media wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Otto Group Media ist die Otto Group Media GmbH, Kleine Rosenstraße 10, 20095 Hamburg, Deutschland. Otto Group Media setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: [https://ottogroup.media/kontakt/datenschutz/](https://ottogroup.media/datenschutz/)

Link zum Opt-Out: Bitte ändern Sie die Präferenzen für Otto Group Media, The ADEX unter <http://www.youronlinechoices.com/de/praferenzmanagement/>  
  
**- Otto (**[**https://www.otto.de**](https://www.otto.de/)**)**

Otto wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Otto ist die Otto (GmbH & Co KG), Werner-Otto-Straße 1-7, 22179 Hamburg, Deutschland. Otto Group Media setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.otto.de/shoppages/service/datenschutz>  
  
Link zum Opt-Out: Bitte ändern Sie die Präferenzen für Otto Group Media, The ADEX unter <http://www.youronlinechoices.com/de/praferenzmanagement/>  
  
**- Adsquare (**[**https://www.adsquare.com/**](https://www.adsquare.com/)**)**

Adsquare wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Adsquare ist die adsquare GmbH, Saarbrücker Str. 36, 10405 Berlin, Deutschland. Adsquare setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.adsquare.com/privacy/>

Link zum Opt-Out: <https://www.adsquare.com/privacy/>  
  
**- iBillboard (**[**https://www.ibillboard.com/en/**](https://www.ibillboard.com/en/)**)**

iBillboard wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von iBillboard ist die Internet BillBoard, a.s., Novoveská 1261/95, 70900, Ostrava, Česká republika. iBillboard setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.ibillboard.com/en/privacy-cookies/>  
  
**- Yieldlove (**[**https://www.yieldlove.com**](https://www.yieldlove.com/)**)**

Yieldlove wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Yieldlove ist die Yieldlove GmbH, Kehrwieder 9, 20457 Hamburg, Deutschland. Yieldlove setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.yieldlove.com/cookie-policy>

Link zum Opt-Out: <https://www.yieldlove.com/cookie-policy>  
  
**- Twiago (**[**https://www.twiago.com/**](https://www.twiago.com/)**)**

Twiago wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Twiago ist die twiago GmbH, Gustav-Heinemann-Ufer 72b, 50968 Köln, Deutschland. Twiago setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.twiago.com/datenschutz/>

Link zum Opt-Out: [http://control.twiago.com/privacy.php](http://control.twiago.com/privacy.php?lang=0)  
  
**- Seeding Alliance (**[**https://seeding-alliance.de/**](https://seeding-alliance.de/)**)**

Seeding Alliance wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Seeding Alliance ist die Seeding Alliance GmbH, Wichernstr. 34b, 21335 Lüneburg, Deutschland. Seeding Alliance setzt Technologien ein, um die Einblendung von Werbemitteln für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://seeding-alliance.de/datenschutz/>

Link zum Opt-Out: <https://seeding-alliance.de/opt-out/>  
  
**- The Tradedesk (**[**https://www.thetradedesk.com/**](https://www.thetradedesk.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von The Tradedesk ist The Trade Desk, Inc, Große Theaterstraße 31, 1st Floor, 20354 Hamburg, Deutschland. The Tradedesk ist eine Plattform für einfaches und transparentes Handling von Werbekampagnen im Real Time & Data Driven Advertising Umfeld.

Link Datenschutzhinweise: <https://www.adition.com/datenschutz/>

Link zum Opt-Out: <https://www.adition.com/datenschutz-opted-out/>  
  
**- Active Agent (**[**https://www.adition.com/produktloesungen/demand-side-platform-dsp/**](https://www.adition.com/produktloesungen/demand-side-platform-dsp/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Active Agent ist Active Agent AG, Ellen-Gottlieb-Straße 16, 79106 Freiburg i.Br., Deutschland. Active Agent ist eine Plattform für einfaches und transparentes Handling von Werbekampagnen im Real Time & Data Driven Advertising Umfeld.

Link Datenschutzhinweise: <https://www.adition.com/datenschutz/>

Link zum Opt-Out: <https://www.adition.com/datenschutz-opted-out/>  
  
**- AdForm (**[**https://site.adform.com/**](https://site.adform.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von AdForm ist die AdForm GmbH, Gr. Burstah 50-52, 20457 Hamburg, Deutschland. Adform setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://site.adform.com/privacy-center/platform-privacy/>

Link zum Opt-Out: [https://site.adform.com/privacy-policy-opt-out/](https://site.adform.com/privacy-center/platform-privacy/opt-out/)  
  
**- Adition (**[**https://www.adition.com/**](https://www.adition.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Adition ist die Adition technologies AG, Am Gatherhof 44, 40472 Düsseldorf, Deutschland. Adition setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.adition.com/datenschutz/>

Link zum Opt-Out: <https://www.adition.com/datenschutz/>  
  
**- Teads (**[**https://www.teads.com/**](https://www.teads.com/)**)**

Teads wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Teads ist die Teads Deutschland GmbH, Poststraße 6, 20354 Hamburg, Deutschland. Teads setzt Technologien ein, um die Einblendung von Werbemitteln, für den User auszusteuern und zu optimieren.

Link Datenschutzhinweise: <https://www.teads.com/privacy-policy/>

Link zum Opt-Out: <https://www.teads.com/privacy-policy/>  
  
-**Integral (**[**https://integralads.com/**](https://integralads.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Integral ist die Integral Ad Science GmbH, Rosenthaler Straße 38, 10178 Berlin, Deutschland. Integral setzt Analyse-Cookies ein, um das Nutzungsverhalten (z. B. geklickte Werbebanner, besuchte Unterseiten, Dauer der Video-Nutzung) unserer Nutzer aufzeichnen und in statistischer Form auswerten und validieren zu können.

Link Datenschutzhinweise: <https://integralads.com/cookie-policy/>

Link zum Opt-Out: <https://integralads.com/cookie-policy/>  
  
**- Appnexus (**[**https://www.xandr.com/**](https://www.xandr.com/)**)**

Appnexus wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Appnexus ist AppNexus Group, 28 W. 23rd Street, 10010 New York, United States. AppNexus setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen zu präsentieren.

Link Datenschutzhinweise: <https://www.xandr.com/privacy/>

Link zum Opt-Out: <https://www.xandr.com/privacy/platform-privacy-policy/#choices>  
  
**- Permodo (**[**https://permodo.com/de.html**](http://https/permodo.com/de.html)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Permodo ist die PERMODO GmbH, Dachauerstrasse 15c, 80335 München, Deutschland. Permodo verarbeitet sogenannte Identifier zur Ausspielung von personalisierter Werbung.

Link Datenschutzhinweise: <https://permodo.com/de/privacy.html>

Link zum Opt-Out: <https://permodo.com/optout/cookieOptOut.php>  
  
**- Neustar (**[**https://www.marketing.neustar/**](https://www.home.neustar/marketing-solutions)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist Neustar, Inc., 21575 Ridgetop Circle, Sterling, VA 20166, USA. Neustar ist ein Anbieter für Data-Management Lösungen und Technologien zur Steuerung von nutzungsbasierten Werbeeinblendungen.

Link Datenschutzhinweise: <https://www.home.neustar/privacy>

Link zum Opt-Out: <https://www.home.neustar/privacy/opt-out>  
  
**- meetrics (**[**https://www.meetrics.com**](https://www.meetrics.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Meetrics ist die Meetrics GmbH, Alexanderstraße 7 in 10178 Berlin, Deutschland. Meetrics setzt Analyse-Cookies ein, um das Nutzungsverhalten (z. B. geklickte Werbebanner, besuchte Unterseiten, Dauer der Video-Nutzung) unserer Nutzer aufzeichnen und in statistischer Form auswerten und validieren zu können

Link Datenschutzhinweise: <https://www.meetrics.com/datenschutz/>  
  
Chrome User: <https://chrome.google.com/webstore/detail/meetrics-optout/kghcchdcafccddoihjihdeoacllhlenh>

FireFox Users: <https://addons.mozilla.org/en/firefox/addon/meetrics-optout/>

**- Ströer SSP (**[**https://www.stroeer.de/konvergenz-konzepte/daten-technologien/stroeer-ssp.html**](https://www.stroeer.de/konvergenz-konzepte/daten-technologien/stroeer-ssp.html)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist die Ströer SSP GmbH, St.-Martin-Str. 106, 81669 München, Deutschland. Die Ströer SSP stellt Online-Marketing-Lösungen bereit, insbesondere im Bereich Adserving, Auslieferung von Werbemitteln und als Marktplatz für digitale Werbemittel.

Link Datenschutzhinweise: <https://www.stroeer.de/service/datenschutz.html>

Link zum Opt-Out: <https://www.stroeer.de/index.php?id=4293>  
  
**- criteo (**[**https://www.criteo.com/de/**](https://www.criteo.com/de/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist Criteo SA, 32 Rue Blanche, 75009 Paris, Frankreich. Criteo setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen zu präsentieren.

Link Datenschutzhinweise: <https://www.criteo.com/de/privacy/>

Link zum Opt-Out: <https://www.criteo.com/de/privacy/>  
  
**- mbr targeting (**[**https://mbr-targeting.com/**](https://mbr-targeting.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist die mbr targeting GmbH, Hobrechtstr. 65, 12047 Berlin, Deutschland. mbr targeting ist ein Anbieter für Data-Management Lösungen und Steuerung von nutzungsbasierten Werbeeinblendungen.

Link Datenschutzhinweise: <https://privacy.mbr-targeting.com/?optedIn=true>

Link zum Opt-Out: <https://privacy.mbr-targeting.com/?optedIn=true>  
  
**- Ströer Digital Media GmbH (**[**https://www.stroeer.de/digitale-werbung.html**](https://www.stroeer.de/digitale-werbung.html)**)**

Betreibt die Auslieferung und Vermarktung von Werbeplätzen auf dem online Angebot mit Zustimmung der Seitenbetreiber. Anbieter ist die Ströer Digital Media GmbH, Kehrwieder 8-9 . 20457 Hamburg

Link Datenschutzhinweise: <https://www.stroeer.de/digitale-werbung/werbemedien/targeting-data/datenschutz.html>  
  
**- DoubleClick for Publishers (**[**https://marketingplatform.google.com/about/enterprise/**](https://marketingplatform.google.com/about/enterprise/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist DoubleClick by Google, a division of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. DoubleClick stellt Online-Marketing-Lösungen bereit, insbesondere im Bereich Adserving, Auslieferung von Werbemitteln und als Marktplatz für digitale Werbemittel.

Link Datenschutzhinweise: <https://policies.google.com/privacy>

Link zum Opt-Out: <https://adssettings.google.com/authenticated?hl=en>  
  
**- DoubleClick Ad Exchange (https://www.doubleclickbygoogle.com/de/solutions/digital-marketing/ad-exchange/)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist DoubleClick by Google, a division of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google stellt Online-Marketing-Lösungen bereit, insbesondere im Bereich Adserving, Auslieferung von Werbemitteln und als Marktplatz für digitale Werbemittel.

Link Datenschutzhinweise: <https://policies.google.com/privacy>

Link zum Opt-Out: <https://adssettings.google.com/authenticated?hl=en>  
  
**- DoubleClick AdSense (**[**https://www.google.de/adsense/start/**](http://https/www.google.de/adsense/start/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist DoubleClick by Google, a division of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google stellt Online-Marketing-Lösungen bereit, insbesondere im Bereich Adserving, Auslieferung von Werbemitteln und als Marktplatz für digitale Werbemittel.

Link Datenschutzhinweise: <https://policies.google.com/privacy>

Link zum Opt-Out: <https://support.google.com/ads/answer/2662922?hl=de>  
  
**- DoubleClick Bid Manager (https://www.doubleclickbygoogle.com/solutions/digital-marketing/bid-manager/)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter ist DoubleClick by Google, a division of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google stellt Online-Marketing-Lösungen bereit, insbesondere im Bereich Adserving, Auslieferung von Werbemitteln und als Marktplatz für digitale Werbemittel.

Link Datenschutzhinweise: <https://policies.google.com/privacy>

Link zum Opt-Out: [https://adssettings.google.com/authenticated?hl=en](http://https/adssettings.google.com/authenticated?hl=en)  
  
**- The Adex/Batch (**[**https://theadex.com/**](https://theadex.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von The ADEX/Batch ist The ADEX GmbH, Torstraße 19, 10119 Berlin, Deutschland. The Adex ist ein Anbieter für Data-Management Lösungen.

Link Datenschutzhinweise: <https://theadex.com/privacy-opt-out/#privacy>

Link zum Opt-Out: <https://theadex.com/privacy-opt-out/>  
  
**- Emetriq (**[**https://www.emetriq.com/**](https://www.emetriq.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Emetriq ist die Emetriq GmbH, Steindamm 80, 20099 Hamburg, Deutschland. Emetriq setzt Technologien zur Steuerung von nutzungsbasierten Werbeeinblendungen ein.

Link Datenschutzhinweise: <https://www.emetriq.com/datenschutz/>

Link zum Opt-Out: <https://www.emetriq.com/opt-out/>  
  
**- 4w Marketplace (**[**https://www.4wmarketplace.com/**](https://www.4wmarketplace.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von 4w Marketplace ist 4w MarketPlace S.r.l, Via Giovanni Paolo II n.100, 84084 Fisciano (Salerno), Italy. 4w Marketplace setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen zu präsentieren..

Link Datenschutzhinweise: <https://www.4wmarketplace.com/privacy/>

Link zum Opt-Out: <https://www.home.neustar/privacy/opt-out>  
  
**- District M (**[**https://www.districtm.net/**](https://www.districtm.net/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von DistrictM ist die district m Inc., 5455 de Gaspé Avenue, Suite 730, Montreal, QC H2T 3B3, Canada. DistrictM setzt Technologien zur Steuerung von nutzungsbasierten Werbeeinblendungen ein.

Link Datenschutzhinweise: [https://districtm.net/en/page/platforms-data-and-privacy-policy/](https://www.districtm.net/platforms-data-privacy-policy/)

Link zum Opt-Out: [https://districtm.net/en/page/platforms-data-and-privacy-policy/](https://www.districtm.net/platforms-data-privacy-policy/)  
  
**- Index Exchange (**[**https://de.indexexchange.com/**](https://de.indexexchange.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Index Exchange ist die Index Exchange, Inc., 74 Wingold Avenue, Toronto, Ontario M6B1P5, Canada. Index Exchange setzt Technologien zur Steuerung von nutzungsbasierten Werbeeinblendungen ein.

Link Datenschutzhinweise: <https://de.indexexchange.com/datenschutzerklarung/>

Link zum Opt-Out: <https://optout.networkadvertising.org/?c=1#!%2F>  
  
**- Media.net (**[**https://www.media.net/de/**](https://www.media.net/de/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Media.net ist die Media.net Advertising Ltd., 107/108, DIC Building 5, Dubai Internet City, Dubai, 215028, United Arab Emirates. Index Exchange setzt Technologien zur Steuerung von nutzungsbasierten Werbeeinblendungen ein.

Link Datenschutzhinweise: <https://www.media.net/privacy-policy/>

Link zum Opt-Out: <https://optout.networkadvertising.org/?c=1>  
  
**- ActiveAgent (**[**https://www.adition.com/produktloesungen/demand-side-platform-dsp/**](https://www.adition.com/produktloesungen/demand-side-platform-dsp/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von ActiveAgent ist die Active Agent AG, Ellen-Gottlieb-Straße 16, 79106 Freiburg i.Br., Deutschland. ActiveAgent setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.adition.com/datenschutz/>

Link zum Opt-Out: <https://www.adition.com/datenschutz/>  
  
**- Bidswitch (**[**https://www.bidswitch.com/**](https://www.bidswitch.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Bidswitch ist die Bidswitch GmbH, Bahnhofstrasse 28, 6304 Zug, Schweiz. Bidswitch setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.bidswitch.com/privacy-policy/>

Link zum Opt-Out: <http://x.bidswitch.net/opt-out>  
  
**- Zemanta (**[**https://www.zemanta.com/**](https://www.zemanta.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Zemanta ist die Zemanta Inc. 33 West 17th Street. 9th floor, 10010 New York NY, United States. Zemanta setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.zemanta.com/legal/privacy/>

Link zum Opt-Out: [https://www.zemanta.com/opt-out](https://www.zemanta.com/opt-out/)  
  
**- Ad Up (**[**https://www.adup-tech.com/**](https://www.adup-tech.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Ad Up ist die Axel Springer Teaser Ad GmbH, Axel-Springer-Straße 65, 10888 Berlin, Deutschland. Ad Up setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.adup-tech.com/>

Link zum Opt-Out: <https://www.adup-tech.com/privacy>  
  
**- LiquidM (**[**https://liquidm.com/**](https://liquidm.com/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von LiquidM ist die LiquidM Technology GmbH, Rosenthalerstr. 36, 10178 Berlin, Deutschland. LiquidM setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://liquidm.com/privacy-policy/>

Link zum Opt-Out: <https://liquidm.com/optout/>  
  
**- RTB House (**[**https://www.rtbhouse.com/de**](https://www.rtbhouse.com/de/)**)**

Wird eingesetzt durch Kunden des digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von RTB House ist die RTB House GmbH, Kurfürstendamm 226, 10719 Berlin, Deutschland. RTB House setzt Technologien ein, um Ihnen für Sie relevante Werbeanzeigen auszuliefern.

Link Datenschutzhinweise: <https://www.rtbhouse.com/privacy-center/>

Link zum Opt-Out: <https://www.rtbhouse.com/de/optout-page/>  
  
**- AudienceProject (**[**https://www.audienceproject.com/**](https://www.audienceproject.com/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von AudienceProject ist AudienceProject ApS Ryesgade 3f, 2200 Copenhagen N, Denmark.

Auf dieser Website werden mit der Technologie von AudienceProject Daten zu Markt- und Medienforschungszwecken erhoben.

Link Datenschutzhinweise: <https://privacy.audienceproject.com/de-DE/for-users/privacy-policy>

Link zum Opt-Out: <https://privacy.audienceproject.com/de-DE/for-users/opt-out>  
  
**- Consentric (**[**https://www.deutschepost.de/de/c/consentric.html**](https://www.deutschepost.de/de/c/consentric.html)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von Consentric ist die Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn, Deutschland. Die Consentric Technologie der Deutsche Post AG nutzt das Consentric Cookie für die Ermittlung statistischer Kennwerte zur crossmedialen Mediennutzung.

Link Datenschutzhinweise: <https://www.deutschepost.de/de/c/consentric/datenschutz.html>

Link zum Opt-Out: <https://pixel.consentric.de/optout>  
  
**- OS Data Solutions GmbH & Co. KG (**[**https://osdatasolutions.de**](https://osdatasolutions.de/)**)**

Wird eingesetzt durch den digitalen Werbevermarkter Ströer Digital Media GmbH. Anbieter von OS Data Solutions ist die OS Data Solutions GmbH & Co. KG, Am Sandtorkai 37, 20457 Hamburg, Deutschland. OS Data Solutions setzt Technologien zur Steuerung von nutzungsbasierten Werbeeinblendungen ein.

Link Datenschutzhinweise: [https://osdatasolutions.de/datenschutz](https://osdatasolutions.de/datenschutz/)

Link zum Opt-Out: Für den Fall, dass Sie zukünftig keine individualisierte Werbung, die auf durch die OS DS gespeicherten Informationen basiert, mehr angezeigt bekommen möchten, können Sie die folgende Opt-out-Möglichkeit (<https://www.youronlinechoices.com/de/praferenzmanagement/>) in Anspruch nehmen, wobei das Opt-out in Bezug auf den Partner der OS Data Solutions, The ADEX, vorzunehmen ist.

**4.3 Weitere Dienste auf t-online.de / Social Plugins**

**- eMail-Dienst**

Wenn Sie sich bei auf der t-online.de einloggen, werden Sie gebeten, Passwort und Ihre E-Mail-Adresse anzugeben („ **Anmeldedaten**“). Der E-Mail-Dienst @t-online.de und der Login zum E-Mail-Dienst verbleiben weiterhin bei der Deutschen Telekom AG. D.h. die Deutsche Telekom AG ist für die Datenverarbeitung im Zusammenhang mit dem E-Mail-Dienst verantwortlich. Weitere Informationen finden Sie unter <https://www.telekom.de/datenschutzhinweise> und unter [info@telekom.de](mailto:info@telekom.de).  
  
**- Facebook**

Auf unseren Seiten sind Buttons des sozialen Netzwerks Facebook, 1601 South California Avenue, Palo Alto, CA 94304, USA integriert. Die Facebook-Buttons erkennen Sie an dem Facebook-Logo oder dem „Like-Button“ („Gefällt mir“) auf unserer Seite. Eine Übersicht über die Facebook-Buttons finden Sie hier:

<https://developers.facebook.com/docs/plugins/>

Wenn Sie bestimmte Artikel auf unseren Seiten besuchen, wird über das Plugin eine direkte Verbindung zwischen Ihrem Browser und dem Facebook-Server hergestellt. Facebook erhält dadurch die Information, dass Sie mit Ihrer IP-Adresse unsere Seite besucht haben und ob bestimmte Dienste genutzt wurden.  
  
Im Übrigen wird eine Verbindung zu Facebook nur dann hergestellt, wenn Sie den Facebook „Like-Button“ anklicken. Während Sie in Ihrem Facebook-Account eingeloggt sind, können Sie dann die Inhalte unserer Seiten auf Ihrem Facebook-Profil verlinken. Durch Ihre Nutzung des Buttons kann Facebook den Besuch unserer Seiten Ihrem Benutzerkonto zuordnen. Facebook kann bei Anklicken des Buttons außerdem weitere Daten verarbeiten, z.B. einen Cookie setzen, über den Facebook auf anderen Internetseiten, die ebenfalls Facebook-Buttons eingebunden haben, erkennen kann, dass sie bereits auf den Button geklickt haben.  
  
Wenn Sie die Recommendations Bar in Facebook zu Ihren Facebook Anwendungen hinzugefügt haben, veröffentlichen Sie automatisch Ihre Leseaktivität auf Ihrem Facebook-Profil, sobald die Recommendations Bar erscheint. Auf Facebook erfahren dann die Personen, die Sie bei Installation der Anwendung hierzu berechtigt haben, welche Inhalte Sie auf t online.de nutzen. Die einzelnen Einträge sowie die Anwendung der Recommendations Bar können Sie jederzeit auf Facebook wieder deaktivieren.  
  
Zudem ist die Zuordnung eines Seitenabrufs zu ihrem Profil auf Facebook möglich. Wenn Sie Facebook-Buttons anklicken und bei Facebook eingeloggt sind oder sich anschließend bei Facebook einloggen, kann z.B. auf Ihrem Facebook-Profil veröffentlicht werden, bei welchen Inhalten Sie den Button angeklickt haben. Facebook kann so gegebenenfalls weitere Daten erheben und speichern. So können bei Facebook-Nutzerprofile entstehen, die über das hinausgehen, was Sie selbst bei Facebook preisgeben. Wir weisen darauf hin, dass wir als Anbieter von t online.de keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch Facebook erhalten. Wir erfahren nicht, wann Sie welchen Button angeklickt haben. Weitere Informationen zur Datennutzung durch Facebook finden Sie in der Datenschutzerklärung von Facebook unter:

<https://de-de.facebook.com/policy.php>  
  
**- Twitter**

Auf unseren Seiten werden außerdem Buttons des Dienstes Twitter genutzt. Diese Buttons werden angeboten durch die Twitter Inc., 795 Folsom St., Suite 600, San Francisco, CA 94107, USA. Sie sind an Begriffen wie “Twitter” oder “Folge”, verbunden mit einem stilisierten blauen Vogel erkennbar. Mit Hilfe der Schaltflächen ist es möglich, einen Beitrag oder eine Seite dieses Angebotes bei Twitter zu teilen oder uns bei Twitter zu folgen.  
  
Wenn Sie bestimmte Artikel unseres Angebots aufrufen, die einen solchen Button enthalten, baut Ihr Browser eine direkte Verbindung mit den Servern von Twitter auf. Der Inhalt des Twitter-Buttons wird von Twitter direkt an Ihren Browser übermittelt. Dabei wird an Twitter übermittelt, dass der entsprechende t online.de Dienst aufgerufen wurde. Auch wenn Sie nicht bei Twitter eingeloggt sind, kann Twitter so gegebenenfalls Nutzungsdaten erheben und speichern.  
  
Im Übrigen wird eine Verbindung zu Twitter nur dann hergestellt, wenn Sie den Twitter-Button anklicken und über das sich öffnende Twitter-Fenster Informationen „twittern“. Dann übermitteln Sie diese Informationen an Twitter, die dann in Ihrem Twitter-Nutzerprofil veröffentlicht werden. Nach unserem Kenntnisstand wird lediglich die IP-Adresse des Nutzers die URL der jeweiligen Webseite beim Bezug des Buttons übermittelt, aber nicht für andere Zwecke, als die Darstellung des Buttons, genutzt. Wir haben jedoch keinen Einfluss auf den Umfang der Daten, die Twitter mit Hilfe dieses Buttons erhebt.  
Weitere Informationen hierzu finden sich in der Datenschutzerklärung von Twitter unter:

[http://twitter.com/privacy](https://twitter.com/de/privacy).  
  
**- Pinterest**

Auf unseren Seiten werden außerdem Buttons des Dienstes Pinterest genutzt. Diese Buttons werden angeboten durch die Pinterest Inc, 505 Brennan St, San Francisco, CA 94103, USA. Sie sind an dem weißen Buchstaben „P“ auf rotem Hintergrund und dem Text „Pinterest“ oder „Pinnen“ erkennbar. Mit Hilfe der Schaltflächen ist es möglich, einen Beitrag oder eine Seite dieses Angebotes bei Pinterest zu teilen oder uns bei Pinterest zu folgen.  
  
Wenn Sie bestimmte Artikel unseres Angebots aufrufen, die einen solchen Button enthalten, baut Ihr Browser eine direkte Verbindung mit den Servern von Pinterest auf. Der Inhalt des Pinterest-Buttons wird von Pinterest direkt an Ihren Browser übermittelt. Dabei wird an Pinterest übermittelt, dass der entsprechende t online.de Dienst aufgerufen wurde. Auch wenn Sie nicht bei Pinterest eingeloggt sind, kann Pinterest so gegebenenfalls Nutzungsdaten erheben und speichern.  
  
Im Übrigen wird eine Verbindung zu Pinterest nur dann hergestellt, wenn Sie den Pinterest-Button anklicken und über das sich öffnende Pinterest-Fenster Informationen teilen. Dann übermitteln Sie diese Informationen an Pinterest, die dann in Ihrem Pinterest-Nutzerprofil veröffentlicht werden. Nach unserem Kenntnisstand wird lediglich die IP-Adresse des Nutzers die URL der jeweiligen Webseite beim Bezug des Buttons übermittelt, aber nicht für andere Zwecke, als die Darstellung des Buttons, genutzt. Wir haben jedoch keinen Einfluss auf den Umfang der Daten, die Pinterest mit Hilfe dieses Buttons erhebt.  
Weitere Informationen hierzu finden sich in der Datenschutzerklärung von Pinterest unter:

[https://policy.pinterest.com/de/privacy-policy.](https://policy.pinterest.com/de/privacy-policy)

**5. Kontakt, Geltendmachung Ihrer Rechte**

Um Ihre vorstehenden Rechte wahrzunehmen oder bei Fragen oder Anmerkungen zu dieser Datenschutzerklärung oder allgemein zum Datenschutz, wenden Sie sich bitte an:

Ströer Digital Publishing  
Platz der Einheit 1  
60327 Frankfurt  
[sdp-datenschutz@stroeer.de](mailto:sdp-datenschutz@stroeer.de)

Sie können sich auch unmittelbar an unseren Datenschutzbeauftragten wenden, welcher in Beschwerdefällen zuständig ist. Sie erreichen ihn unter folgender E-Mail-Adresse: [datenschutzbeauftragter@stroeer.de](mailto:datenschutzbeauftragter@stroeer.de).

Sie haben zudem, wenn wir Ihr Anliegen aus Ihrer Sicht nicht angemessen behandeln u.a. (unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs) ein Beschwerderecht bei der für den Datenschutz zuständigen Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes.

**6. Wie oft aktualisieren wir diese Datenschutzhinweise?**

Wir überarbeiten diese Datenschutzhinweise bei Änderungen an unserer Webseite t-online.de oder bei sonstigen Anlässen, die dies erforderlich machen. Die jeweils aktuelle Fassung finden Sie stets auf dieser Seite.

New York Times

This policy describes how we handle your data when you use “Times Services,” listed below:

* The New York Times newspaper, plus our International Edition
* Our websites, *like nytimes.com*
* Our apps, *like the New York Times app and the New York Times Crossword app*
* Our email newsletters, *like Cooking and Morning Briefing*
* Our pages or ads on social media networks, *like our Facebook and Instagram pages*
* Anywhere we gather information from you and refer you to this Privacy Policy

How we handle information about you depends on which Times Services you use — and how you use them. We use different information about print subscribers than website visitors.

Be aware that certain Times Services work differently. Some have additional terms that supplement this policy *(e.g.,*[*Reader Submissions*](https://help.nytimes.com/hc/en-us/articles/360004901454-Reader-submission-terms)*)*. Others refer to a different privacy policy altogether, so this one does not apply.

**1.**

**What Information Do We Gather About You?**

The information we gather about you depends on the context. By and large, it’s information about you that can personally identify you — either on its own or when combined with other information.

The following describes the information we collect and how we obtain it.

***A) Information Collected Through Times Services.***

1. **Information That You Voluntarily Give Us**
   * **For Registration:**

When you sign up for a Times Service *(e.g., a subscription)*, we collect your contact information and account credentials. Once you’re registered, we assign you a unique ID number. This ID number helps us recognize you when you’re signed in.

For some Times Services, you can instead sign up by linking your Apple, Facebook or Google account. See “[From Other Sources](https://www.nytimes.com/privacy/privacy-policy#anchor-question1-sectionB)” below.

If you register for an event or conference, we might ask for additional information *(e.g., your company name, your job title or your dietary restrictions)*.

* + **For Billing:**

To process payments or donations, we collect and use your payment information.

This can include your name, your address, your telephone number, your email address, your credit or debit card information and any other relevant information.

* + **For User-Generated Content:**

We offer you the ability to post content that other users can read *(e.g., comments or recipe reviews)*. Anyone can read, collect and use any personal information that accompanies your posts. See the [Comments F.A.Q.](https://help.nytimes.com/hc/en-us/articles/115014792387-Comments), or read “[User-Generated Content](https://help.nytimes.com/hc/en-us/articles/115014893428-Terms-of-service#3)” in our Terms of Service for more information.

We do not have to publish any of your content. If the law requires us to take down, remove or edit your personal information, we will comply to the required extent.

* + **For Contests, Sweepstakes and Special Offers:**

When you sign up for these, you give us your name, email and any other required information.

* + **For Reader Surveys, Research, Panels and Experience Programs:**

We gather information through questionnaires, surveys and feedback programs. We also conduct similar research for advertisers. We ask you for your consent to use this information when you participate in these programs and events.

* + **During Contact With Our Call Centers:**

We collect information from you when you place an order over the phone or contact customer service through one of our toll-free numbers.

* + **Personal Contacts Data:**

We never scan your device for your contacts or upload this data.

With your consent, we do comply with your requests to collect data about your friends, family or acquaintances *(e.g., Refer a Friend campaigns)*. This functionality is only meant for U.S. residents. By using it, you acknowledge and agree that both you and your contacts are based in the United States — and that you have everyone’s consent for us to use their contact information.

1. **Information Collected Automatically**
   * **With Tracking Technologies in Your Browser and Mobile Apps:**

These technologies include cookies, web beacons, tags and scripts, software development kits (or SDKs) and beyond.

We track and store data about how you visit and use Times Services, particularly through our websites and apps. The items we log include:

* + - Your IP address
    - Your location
    - Your operating system
    - Your browser
    - Your browser language
    - The URLs of any pages you visit on our sites and apps
    - Device identifiers
    - Advertising identifiers
    - Other usage information.

We combine this data with other information we collect about you. For more information about tracking methods on Times Services, and how to manage them, read our [Cookie Policy](https://www.nytimes.com/subscription/dg-cookie-policy/cookie-policy.html).

If your browser doesn’t accept our cookies, you can’t access certain parts of our websites *(e.g., your account on nytimes.com)*. Because the “Do Not Track” browser-based standard signal has yet to gain widespread acceptance, we don’t currently respond to those signals.

* + **With GPS Technologies:**

Some of our apps can provide content based on your GPS location, if you enable this feature *(e.g., the New York Times Real Estate app)*. Your GPS location is your exact location.

You choose whether to enable GPS features when you first install the app. You can edit that setting on your device at any time. If you enable these features, your GPS location can be found by satellite, cell phone tower or Wi-Fi and used by the app. If you save a location-based search in your history, that data moves to our service provider’s servers — see [below](https://www.nytimes.com/privacy/privacy-policy#anchor-question2-sectionE) for the definition of service provider.

If you do not enable GPS location-based services, or if a specific app does not have location-based features *(e.g., the New York Times app)*, we don’t collect your precise GPS location. We do collect your IP address, which can establish your approximate location. Ads on our sites and apps may be targeted based on this approximate location, but are never targeted based on your GPS location.

***B) Information Collected From Other Sources.***

1. **Privately Owned Databases:**

Marketing, data analytic and social media-owned databases give us access to a range of information — like public data, survey data and beyond. This data sometimes includes your mailing address, your gender, your age, your household income and other demographic data.

1. **Social Media Platforms and Other Third-Party Services:**

*(Social media platforms include Facebook. Third-party services include Google, Kindle and Nook.)*

You can link your social media or other third-party account to a Times Service. By linking the services, you authorize us to collect, store and use any information they may give us *(e.g., your email address)*. You can disconnect your nytimes.com registration from third-party accounts at any time.

We also receive information from you when you interact with our pages, groups, accounts or posts on social media platforms. This includes aggregate data on our followers *(e.g., age, gender and location)*, engagement data *(e.g., “likes,” comments, shares, reposts and clicks)*, awareness data *(e.g., number of impressions and reach)* and individual users’ public profiles.

For more information, refer to our [social login](https://help.nytimes.com/hc/en-us/articles/115014887628-Social-login), [Kindle](https://help.nytimes.com/hc/en-us/articles/115014889068-Kindle-subscribers) and [Nook](https://help.nytimes.com/hc/en-us/articles/115014917867-NOOK-subscribers) F.A.Q.

1. **Workplace and Schools:**

When your employer or school buys an organizationwide subscription to nytimes.com, they sometimes provide us with your name and organization email address to grant you access as a user.

***A note about future updates:***

We are always improving our products and services, and we create new features regularly. These updates sometimes require us to collect new information, or use what we already have differently. If there is a significant or material change in the way we handle your personal information, we will notify you as detailed below.

[**Back to top**](https://www.nytimes.com/privacy/app)

**2.**

**What Do We Do With the Information We Gather?**

***A) We provide the Times Services.***

We use your information to help you use and navigate Times Services, such as:

* Making a Times Service available to you
* Arranging access to your account
* Providing customer service
* Responding to your inquiries, requests, suggestions or complaints
* Completing your payments and transactions
* Sending service-related messages *(e.g., a change in our terms and conditions)*
* Saving your reading list, recipes or property searches
* Displaying your Crossword stats
* Letting you take part in paid services, polls, promotions, surveys, panels, research and comments.

***B) We Personalize Your Experience.***

We track your interests and reading habits *(e.g., the articles you read)* to personalize your reading experience using technology like algorithmic recommendations and machine learning. This is how we highlight articles you might be interested in and de-emphasize articles you’ve already read. For more information about content personalization on Times Services, you can read the [Personalization F.A.Q.](https://help.nytimes.com/hc/en-us/articles/360003965994-Personalization) We also show you prices, promotions, products or services we believe you’ll find interesting, based on demographic and usage data.

***C) We Allow You to Share User-Generated Content.***

Any information you disclose in your content becomes public — along with your chosen screen name and uploaded photo.

***D) We Develop Products and Services, and Do Analysis.***

We analyze data on our users’ subscription, purchase and usage behaviors. This helps us make business and marketing decisions.

For example, our analysis lets us predict preferences and price points for our products and services. It helps us determine whether our marketing is successful. It also shows us characteristics about our readers, which we sometimes share in aggregate with advertisers.

Google Analytics is one of the analytics providers we use. You can find out [how Google Analytics uses data](https://policies.google.com/technologies/partner-sites) and [how to opt out of Google Analytics](https://tools.google.com/dlpage/gaoptout).

***E) We Carry Out Administrative Tasks.***

* For auditing: We verify that our internal processes work as intended and comply with legal, regulatory and contractual requirements.
* For fraud and security monitoring: We detect and prevent cyberattacks or unauthorized robot activities.
* For customer satisfaction: We assess users’ satisfaction with Times Services and our customer care team.

The above activities can involve outside companies, agents or contractors (“service providers”) with whom we share your personal information for these purposes (discussed further below).

***F) We Offer Sweepstakes, Contests and Other Promotions.***

You can take part in our sweepstakes, contests and other promotions. Some might have additional rules about how we use and disclose your personal information.

***G) We Allow for Personalized Advertising on Times Services and Create Audiences for Third Party Advertisers.***

We gather data and work with [third parties](https://www.nytimes.com/privacy/third-party) to show you personalized ads. This data comes from ad tracking technologies set by us or the third party *(e.g., cookies)*, the information you provide *(e.g., your email address)*, your use of Times Services *(e.g., your reading history)*, information from advertisers or advertising vendors *(e.g., demographic data)* and anything inferred from any of this information. We only use or share this information in a manner that does not reveal your identity.

For example, we use Google to serve ads on Times Services. Google uses cookies or unique device identifiers, in combination with their own data, to show you ads based on you visiting nytimes.com and other sites. You can opt out of the use of the Google cookie by visiting the [related Google privacy policy](https://policies.google.com/technologies/ads?hl=en).

We also create specific audiences that allow us to serve you personalized advertising on our sites and apps, on behalf of advertisers. To do this, we combine information we collect through surveys (from subscribers, registered users and non-registered visitors) with information we collect automatically using tracking technologies as you use the Times Services. This combined information is used to build models for measuring users against demographic and interest-based attributes. With the help of service providers, these measurements are then transformed into pools of users grouped by common attributes. Each group is associated with a random ID that is then passed to our ad server for us in targeting advertising campaigns on Times Services.

Another example is our affiliate link vendors, which we use in our guides and product recommendations. Times Services include links that will send you to affiliate vendor URLs and other services not operated or controlled by us. These affiliate vendors use cookies and other technologies to collect information about your navigation from the Times Services to the merchant you are visiting. If you buy a product after following a link to an affiliate link vendor’s URL, we may earn a commission.

***Additional notes:***

* For more about targeted advertising, and how to opt out with your specific browser and device, go to the [DAA Webchoices Browser Check](http://optout.aboutads.info/?c=2&lang=EN) and [NAI Opt Out of Interest-Based Advertising](http://optout.networkadvertising.org/?c=1). You can [download the AppChoices app](https://youradchoices.com/appchoices) to opt out in mobile apps. You can also follow the instructions in the [“What Are Your Rights?”](https://www.nytimes.com/privacy/privacy-policy#anchor-question4) section below.
* We try to limit how our third-party advertising technology vendors use the information they gather from you. Many of these providers require us to enter into contracts that allow them to optimize their own services and products, or that help them create their own.  
    
  Essentially, these providers combine any information they gather about you through Times Services with information they receive from their other clients. This helps them target ads to you on behalf of their other clients, not just us.
* These third parties sometimes use other services in order to serve ads; check [their privacy policies for more details](https://www.nytimes.com/privacy/third-party). For further information on tracking technologies and your rights and choices regarding them, see the applicable [Cookie Policy](https://www.nytimes.com/subscription/dg-cookie-policy/cookie-policy.html).

***H) We Advertise Times Services to You.***

We market our properties to you. Sometimes we use marketing vendors to do this.

We serve ads through websites, locations, platforms and services operated and owned by third parties. Often these ads are targeted at people who have visited or registered for a Times Service but have not subscribed or purchased anything. The ads are also targeted at people with similar traits or behaviors to our subscribers or customers.

We target our advertising to these users by uploading an encrypted customer list to a third party, or by incorporating a tracking technology from a third party onto our Times Service. The third party then matches individuals who appear in both our data and their data. Because of how this matching process works, the third party can’t read our encrypted customer list if they don’t already have it.

To opt out of receiving these matched ads, contact the applicable [third parties](https://www.nytimes.com/privacy/third-party). For example, when we use “Custom Audience” to serve you our ad through Facebook, you should be able to hover over the box in the right corner of that Facebook ad and opt out. We are not responsible for any third party’s failure to comply with opt-out requests.

We periodically send you targeted email newsletters or promotional emails. For information on opting out of these emails, see [“What Are Your Rights?”](https://www.nytimes.com/privacy/privacy-policy#anchor-question4)

***I) We Aggregate (or De-identify) Personal Information Into Larger Findings.***

Sometimes we aggregate or de-identify information so that it can no longer identify you, under applicable laws. This helps us better understand and represent our users, such as when we measure ad performance, create advertising interest-based segments or compile survey results. We can use and disclose this aggregated or de-identified information for any purpose, unless an applicable law says otherwise.

[**Back to top**](https://www.nytimes.com/privacy/app)

**3.**

**With Whom Do We Share the Information We Gather?**

***A) Within The New York Times Company:***

We share your information with our affiliates for the purposes listed here. See [a list of our affiliates](https://help.nytimes.com/hc/en-us/articles/360004990014).

***B) With Service Providers:***

We work with service providers, as defined [above](https://www.nytimes.com/privacy/privacy-policy#anchor-question2-sectionE), to carry out certain tasks:

* Processing your payments
* Fulfilling your orders
* Maintaining technology and related infrastructure
* Offering you customer service
* Serving and targeting ads
* Measuring ad performance
* Presenting surveys
* Shipping you products and mailings
* Distributing emails
* List processing and analytics
* Managing and analyzing research
* Managing promotions

When performing these tasks, service providers often have access to your personal information.

We sometimes allow them to use aggregated or de-identified information for other purposes, in accordance with applicable laws

***C) With Other Third Parties:***

There are situations when we share your information with third parties beyond our service providers. We never share your email address with these third parties without your consent, except in encrypted form to engage in the matched ads process described [above](https://www.nytimes.com/privacy/privacy-policy#anchor-question2-sectionH).

1. If you’re a U.S. print subscriber, we may share your name and mailing address (among other information) with other reputable companies that want to market to you by mail.
2. We share information about our live event and conference attendees *(e.g., your name, your company or your job title)* with the event sponsors. In those cases we notify you when you provide us the information.
3. We share information about participants in our sweepstakes, contests and similar promotions with the promotions’ sponsors. In those cases we notify you when you provide us the information.
4. We process payments you make through Times Services with external services.

There are two ways this can happen:

* + We collect your information and share it with the third-party service for processing.
  + The third-party service collects your information for processing.

1. In the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings), we would have a legitimate interest in disclosing or transferring your information to a third party — such as an acquiring entity and its advisers.
2. We can preserve or share personal information if the law requires us to do so. We can also preserve or share personal information if we believe it would be necessary to:
   * Comply with the law or with legal process
   * Protect and defend our rights and property
   * Protect against misuse or unauthorized use of the Times Services
   * Protect the safety or property of our users or the general public *(e.g., if you provide false information or attempt to pose as someone else, we could share your information to help investigations into your actions)*
   * Cooperate with government authorities, which could be outside your country of residence.
3. We disclose public activities in our RSS feeds, APIs and other distribution formats. Your public activities could thus appear on other websites, blogs or feeds.

[**Back to top**](https://www.nytimes.com/privacy/app)

**4.**

**What Are Your Rights?**

***A) How Do I Opt Out of Email, Phone, Mail and Push Notifications?***

The opt-out methods described below are limited to the email address, phone or device used. They won’t affect subsequent subscriptions.

1. **Email:**

We offer a variety of commercial emails and email newsletters. You can unsubscribe from them by following the “unsubscribe” instructions near the bottom of the email. You can also email us at [privacy@nytimes.com](mailto:privacy@nytimes.com).

You can [manage your nytimes.com newsletter preferences](https://myaccount.nytimes.com/seg/settings).

1. **Mail or Telephone Promotions:**

You can ask us to unsubscribe from our mail or telephone solicitations. You can also ask us to not share your information with third parties for marketing purposes. To do so, email us at [privacy@nytimes.com](mailto:privacy@nytimes.com) with “Opt Out” in the subject line, and your account number and phone number in the body of the email.

You can write to us at: *Customer Care, P.O. Box 8041, Davenport, IA 52808-8041*— or, for International Edition customers, *The New York Times International Edition, Immeuble Le Lavoisier, 4, Place des Vosges, CS 10001, 92052 Paris La Défense Cedex, France*. Please include your account number and phone number in the body of the letter.

1. **Push Notifications:**

You can opt out any time by adjusting your device settings, or uninstalling our app.

1. **Text Messages:**

You can opt out of text alerts any time by replying “STOP,” or any alternative keyword we’ve shared with you.

We complete any opt-out request as quickly as we can. This opt-out request won’t prohibit us from sending you important nonmarketing notices.

***B) How Do You Access, Change, Delete, Update or Exercise Your Other Rights in Relation to Your Personal Information?***  
In some parts of the world, you have the right to:

* Access, modify, or delete the personal information we have about you
* Receive an electronic copy of the personal information we have about you, for data portability
* Restrict, or object to, how we process personal information about you
* Not receive discriminatory treatment by us for the exercise of your privacy rights.

You have the right to object to the processing of your personal information based on our legitimate interest or that of a third party — unless we demonstrate compelling legitimate grounds for the processing of, or the keeping of, your personal information for the establishment, exercise or defense of legal claims.

If you’d like to exercise any of the above rights, contact us via [this form](https://www.nytimes.com/data-subject-request) or by calling us at our toll-free number, 1-800-NYTIMES. In your request, please be specific. State the information you want changed, whether you’d like your information suppressed from our database or whether there are limitations you’d like us to put on how we use your personal information. Please use the email address linked to that personal information — we only complete requests on the information linked to your email address. To verify your identity, we will email the email address you provide us, and which matches our records, and wait for your response. In some instances we may also ask for additional information. This is how we verify your identity before complying.

You can designate an authorized agent to make a request on your behalf. In order to do that, please provide the agent with written permission, signed by you, authorizing the agent to submit the request on your behalf. The agent must submit that written permission along with the request. We will contact you to verify your identity — and the authorized agent’s permission — before a response to the request is sent.

We’ll respond to your request in a manner consistent with applicable law.

We might need to keep certain information for recordkeeping purposes, or to complete a transaction you began prior to requesting a change or deletion *(e.g., if you make a purchase or enter a promotion, you might not be able to change or delete the personal information provided until after the completion of the purchase or promotion)*.

In some cases, your request doesn’t ensure complete removal of the content or information *(e.g., if another user has reposted your content)*.

If you’d like, you can lodge a complaint with a data protection authority. A [list of E.U. data protection authorities](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080) is available.

***C) How Do You Manage Your Digital and Home Delivery Accounts?***

You can update your account information and see [your transaction history](https://myaccount.nytimes.com/) (for [International Edition print subscribers](https://customercare.inyt.com/)). If you need assistance, call our toll-free number, 1-800-NYTIMES. [Other local numbers](https://subscribe.inyt.com/footer?requestAction=displayContactIht) are available.

It works differently if you subscribed via Apple’s App Store or Google Play. Register with us to access the Account area, and contact Apple or Google for your transaction history.

[**Back to top**](https://www.nytimes.com/privacy/app)

**5.**

**What About Sensitive Personal Information?**

We generally don’t want to gather any sensitive information about you. This includes:

* Your social security number
* Your racial or ethnic origin
* Your political opinions
* Your religion or other beliefs
* Your health, biometric or genetic characteristics
* Any trade union membership
* Any criminal background

There are rare situations when we request this information *(e.g., a reader survey asks about your political leanings)*, but you can decline to answer. Outside those situations we would prefer you never share that information with us.

[**Back to top**](https://www.nytimes.com/privacy/app)

**6.**

**How Long Do You Retain Data?**

It depends. We store your personal information for as long as needed, or permitted, based on the reason why we obtained it (consistent with applicable law). This means we might retain your personal information even after you close your account with us.

When deciding how long to keep your information, we consider:

* How long we’ve had a relationship with you or provided a Times Service to you
* Whether we are subject to any legal obligations *(e.g., any laws that require us to keep transaction records for a certain period of time before we can delete them)*
* Whether we have taken any legal positions *(e.g., in connection with any statutes of limitation)*.

Rather than delete your data, we might de-identify it by removing identifying details.

[**Back to top**](https://www.nytimes.com/privacy/app)

**7.**

**How Do You Protect My Information?**

We protect your personal information with a series of organizational, technological and physical safeguards — but we cannot guarantee its absolute security. We recommend that you use complex and unique passwords for your Times accounts and for third-party accounts linked to them. Do not share your password with anyone.

If you have reason to believe your interaction with us is no longer secure, notify us immediately.

[**Back to top**](https://www.nytimes.com/privacy/app)

**8.**

**Are There Guidelines for Children?**

Times Services are intended for a general audience, and are not directed at children under (13) years of age.

We do not knowingly gather personal information (as defined by the U.S. Children’s Privacy Protection Act, or COPPA) in a manner not permitted by COPPA. If you are a parent or guardian and you believe we have collected information from your child in a manner not permitted by law, contact us at [privacy@nytimes.com](mailto:privacy@nytimes.com). We will remove the data to the extent required by applicable laws.

[**Back to top**](https://www.nytimes.com/privacy/app)

**9.**

**How Is Information Transferred Internationally?**

The New York Times Company is headquartered in the United States. If you are located outside the United States, your information is collected in your country and then transferred to the United States — or to another country in which we (or our affiliates or service providers) operate.

If we transfer your data out of the European Economic Area (E.E.A.), we implement at least one of the three following safeguards:

* We transfer your information to countries that have been recognized by the European Commission as providing an adequate level of data protection according to E.E.A. standards (see the [full list of these countries](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)).
* We use a service provider in the United States that is [Privacy Shield](https://www.privacyshield.gov/welcome) certified.
* We take steps to ensure that the recipient is bound by E.U. Standard Contractual Clauses to protect your personal data. You can see a [copy of these clauses](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

In certain situations, the courts, law enforcement agencies, regulatory agencies or security authorities in those countries might be entitled to access your personal information.

[**Back to top**](https://www.nytimes.com/privacy/app)

**10.**

**What Is Our Legal Basis?**

In some jurisdictions, like the European Union and the European Economic Area, we only collect, use or share information about you when we have a valid reason. This is called “lawful basis.” Specifically, this is one of the following:

* The consent you provide to us at the point of collection of your information
* The performance of the contract we have with you
* The compliance of a legal obligation to which we are subject or
* The legitimate interests of The Times, a third party or yourself. “Legitimate interest” is a technical term under international laws, including the European Union General Data Protection Regulation. It means that there are good reasons for the processing of your personal information, and that we take measures to minimize the impact on your privacy rights and interests. “Legitimate interest” also refers to our use of your data in ways you would reasonably expect and that have a minimal privacy impact.

We have a legitimate interest in gathering and processing personal information, for example: (1) to ensure that our networks and information are secure; (2) to administer and generally conduct business within The New York Times Company; (3) to prevent fraud; and (4) to conduct our marketing activities.

[**Back to top**](https://www.nytimes.com/privacy/app)

**11.**

**Links to Third-Party Services?**

Some Times Services contain links to third-party websites, resources, vendors and advertisers. These third parties are not Times Services. We do not control (and are not responsible for) third party content or privacy practices. Any personal data you provide to them is not covered by this Privacy Policy.

[**Back to top**](https://www.nytimes.com/privacy/app)

**12.**

**How Are Changes to This Privacy Policy Communicated?**

We periodically update this Privacy Policy. We will post any changes on this page by updating this policy.

If we make a significant or material change in the way we collect, use or share your personal information, we will notify you at least 30 days prior to the changes taking effect. We will do this via email or prominent notice within Times Services. If you object to any change, you can stop using the Times Services.

After we post any changes on this page, your continued use of Times Services is subject to the updated Privacy Policy.

[**Back to top**](https://www.nytimes.com/privacy/app)

**13.**

**How Can You Contact Us? Who Is the Controller of Your Personal Information?**

If you have any questions, email us at [privacy@nytimes.com](mailto:privacy@nytimes.com) or write us at:

The New York Times Company  
620 Eighth Avenue  
New York, N.Y. 10018  
Attn.: Privacy Counsel

We can also be reached by phone at 1-800-NYTIMES (see [a list of our local telephone numbers outside the United States](https://subscribe.inyt.com/footer?requestAction=displayContactIht)).

The New York Times Company is referred to in this Privacy Policy as “The Times,” “we” or “our.”

Certain Times Services operate as independent controllers of your personal information. Wirecutter operates as an independent controller of personal information collected through the Wirecutter site available at nytimes.com/wirecutter, pages or ads on social media networks, email messages sent by Wirecutter, your offline contacts and any other service offered by Wirecutter (collectively, the “Wirecutter Services”). If you have any questions regarding Wirecutter, email us at [privacy@thewirecutter.com](mailto:privacy@thewirecutter.com) or write us at:

Wirecutter, Inc.  
c/o The New York Times Company  
620 Eighth Avenue  
New York, N.Y. 10018  
Attn.: Privacy Counsel

Wirecutter operates the Wirecutter Services in accordance with the practices disclosed in this Privacy Policy. With respect to the Wirecutter Services, Wirecutter, Inc. is referred to in this Privacy Policy as included in “The Times,” “we” or “our.” In this Privacy Policy, Wirecutter Services are included under “Times Services.”

Amazon

Amazon.de Datenschutzerklärung

Zuletzt geändert: 01. Oktober 2019

Die vorherige Version der Amazon.de Datenschutzerklärung finden Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=GYT8SUSD2E9EWE8Q).

Wir wissen, dass Ihnen der sorgfältige Umgang mit Ihren persönlichen Informationen wichtig ist. Deshalb schätzen wir Ihr Vertrauen, dass Amazon gewissenhaft mit diesen Informationen umgeht. Diese Datenschutzerklärung beschreibt, wie wir Ihre persönlichen Informationen über Amazon-Webseiten, sowie Geräte, Produkte, Dienste, Online- und physische Geschäfte und Anwendungen von Amazon erfassen und verarbeiten, die auf diese Datenschutzerklärung verweisen (zusammen "Amazon Services").

* [Verantwortliche](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_59D17962BEAC4806A83E752ECC5FC54D)
* [EU-US und Schweiz-US Privacy Shield (EU-US Datenschutzschild)](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_1930A607CA354E24B1C8893B4226AB4E)
* [Welche persönlichen Informationen von Kunden erhebt Amazon Europe?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_7C569F52615A45629A7A4922B1CFA46C)
* [Für welche Zwecke verarbeitet Amazon Europe Ihre persönlichen Informationen?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_6CF7F3B544934D8A8F319CABBBEABA16)
* [Was hat es mit Cookies auf sich?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_702C0851FE5042E5AD0C358CAF1A0AE0)
* [Gibt Amazon Europe persönliche Informationen weiter?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_2609CB37E82B4A4991D3BECAE70486B7)
* [Wie sicher sind Informationen über mich?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_26F575D46C974094A0C700AB397EA006)
* [Was hat es mit Werbung von Dritten und Links zu anderen Seiten auf sich?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_9BF94D4200AA4207B2A835DE6B7957FE)
* [Welche Informationen kann ich einsehen?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_384164D5979342509569F0D6B900E5DC)
* [Welche Wahlmöglichkeiten habe ich?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_58728EF7358E4BF093F107D16E3E9451)
* [Dürfen Kinder Amazon Services benutzen?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_8A2B50F690A24C9CB4EC89B95DEDA8A9)
* [Wie lange speichern wir Ihre persönlichen Informationen?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_CC8D0F28BF6544B5937531FB0B44AE58)
* [Kontakte, Hinweise & Änderungen](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE)
* [Verwandte Themen](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_EBFF057433DB42B4B34EE465B1DD2F91)

**Verantwortliche**

Amazon Europe Core S.à.r.l., die Amazon EU S.à.r.l, die Amazon Services Europe S.à.r.l. und die Amazon Media EU S.à.r.l., alle vier ansässig in 38, avenue John F. Kennedy, L-1855 Luxemburg, sowie Amazon Digital Germany GmbH, Domagkstr. 28, 80807 München (zusammen "Amazon Europe") sind Verantwortliche für alle persönlichen Informationen, die von Amazon Europe erhoben und verarbeitet werden. Weitere Informationen finden Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE).

**EU-US und Schweiz-US Privacy Shield (EU-US Datenschutzschild)**

Amazon.com, Inc. nimmt am Programm EU-US und Schweiz-US Privacy Shield ("EU-US Datenschutzschild") teil. Klicken Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_37E3A9F3B10940399940A4F3681DE475), um mehr zu erfahren.

**Welche persönlichen Informationen von Kunden erhebt Amazon Europe?**

Wir erheben Ihre persönlichen Informationen, um Produkte und Dienstleistungen bereitzustellen und kontinuierlich zu verbessern.

Dazu zählen folgende Kategorien von persönlichen Informationen:

1. **Informationen, die Sie uns geben:** Wir erfassen und speichern alle Informationen, die Sie uns im Zusammenhang mit Amazon Services übermitteln. Klicken Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_60E44070B3B74D83B51778D69117FA68), um sich einige Beispiele von Informationen anzusehen, die wir erheben. Sie können entscheiden, uns bestimmte Informationen nicht zur Verfügung zu stellen, was allerdings dazu führen kann, dass Sie viele der Amazon Services nicht nutzen können.
2. **Automatische Informationen:** Sobald Sie Amazon Services nutzen, erhalten und speichern wir automatisch bestimmte Informationen, wie beispielsweise Information bezüglich Ihrer Nutzung, einschließlich Ihrer Interaktion mit Inhalten und Diensten, die über Amazon Services verfügbar sind. Unter anderem verwenden wir - wie viele andere Websites auch - so genannte "Cookies" und andere individuelle Kennungen und erhalten bestimmte Informationen, sobald Ihr Webbrowser oder Ihr Gerät auf Amazon Services und andere Inhalte zugreift, die von oder im Auftrag von Amazon Europe auf anderen Websites bereitgestellt werden. Klicken Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_60E44070B3B74D83B51778D69117FA68), um Beispiele derjenigen Informationen sehen zu können, die wir erheben.
3. **Informationen aus anderen Quellen:** Gelegentlich nutzen wir auch Informationen über Sie aus anderen Quellen. Klicken Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_60E44070B3B74D83B51778D69117FA68), um Beispiele für Informationen zu sehen, die wir erhalten.

**Für welche Zwecke verarbeitet Amazon Europe Ihre persönlichen Informationen?**

***Wir verarbeiten Ihre persönlichen Informationen, um die Amazon Services zu betreiben, bereitzustellen und zu verbessern, die wir unseren Kunden anbieten. Zu diesen Zwecken zählen:***

* **Kauf und Lieferung von Produkten und Dienstleistungen.** Wir verwenden Ihre persönlichen Informationen, um Bestellungen entgegenzunehmen und abzuwickeln, Produkte und Dienstleistungen zu liefern, Zahlungen abzuwickeln und mit Ihnen über Bestellungen, Produkte, Dienstleistungen und Werbeangebote zu kommunizieren.
* **Bereitstellung, Fehlerbehebung und Verbesserung der Amazon Services.** Wir nutzen Ihre persönlichen Informationen, um Funktionen bereitzustellen, Leistungen zu analysieren, Fehler zu beheben und die Benutzerfreundlichkeit und Effektivität der Amazon Services zu verbessern.
* **Empfehlungen und Personalisierung.** Wir verarbeiten Ihre persönlichen Informationen, um Funktionen, Produkte und Dienstleistungen zu empfehlen, die für Sie von Interesse sein könnten, um Ihre Präferenzen zu ermitteln und Ihre Erfahrungen mit Amazon Services zu personalisieren.
* **Bereitstellung von Sprachdiensten.** Wenn Sie Sprachdienste nutzen, verarbeiten wir Ihre Spracheingabe und andere persönliche Informationen, um auf Ihre Anfragen zu antworten, Ihnen den gewünschten Dienst zu erbringen und die Amazon Services Angebote zu verbessern. Für weitere Informationen über Alexa Sprachdienste, klicken Sie [hier](https://www.amazon.de/help/AlexaPrivacy).
* **Einhaltung rechtlicher Verpflichtungen.** In bestimmten Fällen unterliegen wir rechtlichen Verpflichtungen, Ihre persönlichen Informationen zu erheben und zu verarbeiten. Zum Beispiel sammeln wir von Verkäufern Informationen bezüglich des Sitzes und ihren Bankkontoinformationen zum Zwecke der Identitätsprüfung und zu weiteren Zwecke.
* **Kommunikation mit Ihnen.** Wir verwenden Ihre persönlichen Informationen, um mit Ihnen über verschiedene Kanäle (z.B. per Telefon, E-Mail, Chat) bezüglich Amazon Services zu kommunizieren.
* **Anzeigen.** Wir verwenden Informationen wie Ihre Interaktionen mit Amazon Websites, Inhalte oder Dienstleistungen, um interessenbezogene Anzeigen für Funktionen, Produkte und Dienstleistungen zu schalten, die für Sie von Interesse sein könnten. Wir verwenden keine Informationen, die Sie persönlich identifizieren, zur Anzeige interessenbasierter Werbung. Um mehr zu erfahren, lesen Sie bitte unsere [Hinweise zur interessenbasierten Werbung](https://www.amazon.de/gp/help/customer/display.html/?nodeId=201909150).
* **Betrugsprävention und Kreditrisiken.** Wir verarbeiten persönliche Informationen, um Betrug und Missbrauch zu verhindern oder aufzudecken, um die Sicherheit unserer Kunden, von Amazon Europe und Dritten zu schützen. Zur Bewertung von und dem Umgang mit Kreditrisiken setzen wir gegebenenfalls auch Scoring-Verfahren ein.
* **Zwecke, für die wir Ihre Einwilligung einholen.** Eventuell bitten wir Sie um Ihre Einwilligung, Ihre persönlichen Informationen für einen speziellen Zweck zu verarbeiten, den wir Ihnen mitteilen werden. Wenn Sie in die Verarbeitung Ihrer persönlichen Informationen zu einem bestimmten Zweck einwilligen, können Sie Ihre Einwilligung jederzeit frei widerrufen und wir werden die Verarbeitung Ihrer Informationen zu diesem Zweck einstellen.

**Was hat es mit Cookies auf sich?**

Um unseren Systemen zu ermöglichen, das von Ihnen genutzte Endgerät oder den von Ihnen genutzten Browser zu erkennen und Ihnen die Amazon Services erbringen zu können, nutzen wir Cookies. Weitere Informationen über Cookies und wie wir diese einsetzen, lesen Sie bitte unsere [Hinweise zu Cookies](https://www.amazon.de/gp/help/customer/display.html/?nodeId=201890250).

**Gibt Amazon Europe persönliche Informationen weiter?**

Informationen über unsere Kunden sind ein wichtiger Teil unseres Geschäfts. Es gehört jedoch nicht zu unserem Geschäft, die persönlichen Informationen unserer Kunden zu verkaufen. Wir geben persönliche Informationen von Kunden ausschließlich in dem im Folgenden beschriebenen Umfang und ausschließlich an Amazon.com, Inc. und an Tochtergesellschaften, die von Amazon.com, Inc. beherrscht werden weiter, die entweder dieser Datenschutzerklärung unterliegen oder Maßnahmen umsetzen, die mindestens ebenso viel Schutz bieten wie die in dieser Datenschutzerklärung beschriebenen:

* **Transaktionen mit Dritten:** Wir stellen Ihnen Dienste, Produkte, Apps oder Skills zur Verfügung, die von Dritten zur Nutzung auf oder durch Amazon Services bereitgestellt werden. Sie können beispielsweise Produkte von Drittanbietern über unsere Einzelhandelswebsites bestellen, Apps von Drittanbietern aus unserem App Store herunterladen und die Skills von Drittanbietern über unseren Alexa Sprachdienst aktivieren. In einigen Fällen erbringen wir Dienstleistungen oder verkaufen Produktlinien gemeinsam mit Drittanbietern, wie z.B. Co-Branding-Kreditkarten. Sie wissen stets, ob ein dritter Partner an Transaktionen beteiligt ist und ob wir Informationen im Zusammenhang mit dieser Transaktionen an diesen Partner weitergeben werden.
* **Drittdienstleister:** Wir beauftragen andere Unternehmen und Einzelpersonen mit der Erfüllung von Aufgaben für uns. Beispiele sind u. a. die Erfüllung von Bestellungen von Produkten und Dienstleistungen, Paketlieferung, Sendung von Briefen oder E-Mails, die Pflege unserer Kundenlisten, die Analyse unserer Datenbanken, Unterstützung bei Werbemaßnahmen, die Bereitstellung von Suchergebnissen und Links (einschließlich bezahlter Angebote und Links), Abwicklung von Zahlungen (Kreditkarte, Lastschriftverfahren und Rechnungskauf), Übermittlung von Inhalten, Bewertung von Kreditrisiken sowie Kundenservice. Diese Drittdienstleister haben Zugang zu persönlichen Informationen, die zur Erfüllung ihrer Aufgaben benötigt werden. Sie dürfen diese jedoch nicht zu anderen Zwecken verwenden. Darüber hinaus sind sie verpflichtet, die Informationen gemäß dieser Datenschutzerklärung sowie den einschlägigen Datenschutzgesetzen zu behandeln.
* **Übertragung von Geschäftsanteilen:** Da wir unser Geschäft ständig weiterentwickeln, kann es sein, dass wir andere Unternehmen oder Dienstleistungen verkaufen oder kaufen. Bei solchen Transaktionen werden die Kundeninformationen gewöhnlich zusammen mit dem zu übertragenden Teil des Unternehmens übertragen. Diese Informationen unterliegen jedoch auch weiterhin den vorher bestehenden Datenschutzerklärungen (ausgenommen hiervon ist selbstverständlich der Fall, in dem der Kunde anderen Bestimmungen ausdrücklich zustimmt). In dem unwahrscheinlichen Fall, dass Amazon.com, Inc. insgesamt oder die wesentlichen Teile davon verkauft werden, werden persönliche Informationen an den Käufer weitergegeben.
* **Schutz von Amazon Europe und Dritten:** Wir geben Kundenkonten und persönliche Informationen über Kunden bekannt, wenn wir hierzu gesetzlich verpflichtet sind oder wenn eine solche Weitergabe erforderlich ist, um unsere [Allgemeinen Geschäftsbedingungen](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909000) oder andere Vereinbarungen durchzusetzen oder die Rechte von Amazon Europe, sowie die Rechte unserer Kunden und von Dritten zu schützen. Dies beinhaltet einen Datenaustausch mit Unternehmen zur Vorbeugung und Minimierung von Missbrauch und Kreditkartenbetrug.

In allen anderen Fällen werden wir Sie darüber informieren, wenn persönliche Informationen an Dritte weitergegeben werden sollen. So haben Sie die Möglichkeit zu entscheiden, dass Ihre Informationen nicht mit dem Dritten geteilt werden sollen.

**Datenübermittlung an Länder außerhalb des Europäischen Wirtschaftsraums:** Bei der Weitergabe persönlicher Informationen an Dritte in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) stellen wir immer sicher, dass die Übermittlung der Informationen in Übereinstimmung mit dieser Datenschutzerklärung und den anwendbaren Datenschutzgesetzen erfolgt.

**Wie sicher sind Informationen über mich?**

Bei der Entwicklung unserer Systeme und Geräte berücksichtigen wir Ihre Sicherheit und Privatsphäre.

* Um die Sicherheit Ihrer Informationen bei Übertragung zu schützen, benutzen wir Secure Sockets Layer Software (SSL). Diese Software verschlüsselt die Informationen, die von Ihnen übermittelt werden.
* Beim Umgang mit Kreditkarten befolgen wir den Payment Card Industry Data Security Standard (PCI DSS).
* Wir unterhalten physische, elektronische und verfahrenstechnische Sicherheitsmaßnahmen im Zusammenhang mit der Erhebung, dem Speichern und der Offenlegung von persönlichen Informationen unserer Kunden. Diese Sicherheitsmaßnahmen beinhalten, dass wir Sie gelegentlich darum bitten, einen Nachweis über Ihre Identität zu erbringen, bevor wir Ihnen persönliche Informationen offenlegen.
* Unsere Geräte bieten Sicherheitsfunktionen zum Schutz vor unberechtigtem Zugriff und Datenverlust. Sie können diese Funktionen steuern und nach Ihren Bedürfnissen konfigurieren. Klicken Sie [hier](https://www.amazon.com/devicesupport) für weitere Informationen zur Verwaltung der Sicherheitseinstellungen Ihres Geräts.
* Für Sie ist es wichtig, sich gegen unbefugten Zugang zu Ihrem Passwort, Ihren Computern, Geräten und Apps zu schützen. Wenn Sie Ihren Computer mit anderen teilen, sollten Sie darauf achten, sich nach jeder Sitzung [abzumelden](https://www.amazon.de/gp/help/customer/display.html?nodeId=GX7AZREFL3D5VC2D).

**Was hat es mit Werbung von Dritten und Links zu anderen Seiten auf sich?**

Amazon Services beinhaltet Werbung von Dritten und Links zu anderen Webseiten und Apps. Dritte, die Werbepartner sind, können Informationen über Sie sammeln, wenn Sie mit deren Inhalten, Werbung und Dienstleistungen interagieren. Weitere Informationen über Werbung von Dritten auf Amazon Europe, inkl. interessenbasierter Anzeigen, finden Sie in unseren [Hinweisen zu interessenbasierter Werbung](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909150). [Hier](https://www.amazon.de/adprefs) können Sie Ihre Werbungseinstellungen anpassen. Für Informationen, wie Sie auf Ihre persönlichen Informationen zugreifen können, klicken Sie [hier](https://www.amazon.de/privacy) .

**Welche Informationen kann ich einsehen?**

Sie können Ihre Informationen in dem Bereich "Mein Konto" auf unserer Website einsehen. Diese Informationen beinhalten Ihren Namen, Ihre Adresse, Zahlungsoptionen, Profilinformationen, Informationen bezüglich der Prime-Mitgliedschaft, Haushaltseinstellungen und Ihre vergangenen Bestellungen. Um eine Liste mit Beispielen zu sehen, auf die Sie zugreifen können, klicken Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_8E8555298F744144B56A48C866F09067).

**Welche Wahlmöglichkeiten habe ich?**

Wenn Sie Fragen oder Einwände bezüglich der Art haben, wie wir Ihre persönlichen Informationen erfassen und verarbeiten, wenden Sie sich bitte an unseren [Kundenservice](https://www.amazon.de/kontakt). Viele unserer Amazon Services enthalten auch Einstellungen, die Ihnen verschiedene Auswahlmöglichkeiten für die Verwendung Ihrer Informationen bieten.

* Wie oben dargelegt, steht es Ihnen offen, bestimmte Informationen nicht zur Verfügung zu stellen. In diesem Fall können Sie dann aber die Vorteile von vielen der Amazon Services nicht nutzen.
* Auf den unter "[Informationen, zu denen Sie Zugang haben](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_8E8555298F744144B56A48C866F09067)" bezeichneten Seiten können Sie bestimmte Informationen hinzufügen oder aktualisieren. Wenn Sie Informationen aktualisieren, behalten wir gewöhnlich eine Kopie Ihrer ursprünglichen Angaben in unseren Unterlagen.
* Sie können Ihr [Benutzerkonto](https://www.amazon.de/gp/gss/ccp/) entsprechend anpassen, wenn Sie keine E-Mails oder andere Nachrichten von uns erhalten wollen. Möchten Sie keine In-App Benachrichtigungen von uns erhalten, passen Sie bitte Ihre Benachrichtigungseinstellungen in der App auf Ihrem Gerät an.
* Wenn Sie interessenbasierte Werbung sehen möchten, [ändern Sie bitte Ihre Werbungseinstellungen](https://www.amazon.de/gp/dra/info).
* Die Hilfe-Funktion in der Menüleiste der meisten Webbrowser und Geräte erklärt Ihnen, wie Sie Ihren Browser oder Ihr Gerät davon abhalten, neue Cookies zu akzeptieren, wie Sie Ihren Browser Sie darauf hinweisen lassen können, wenn Sie ein neues Cookie erhalten oder auch wie Sie sämtliche Cookies ausschalten. Da Ihnen Cookies ermöglichen, einige wesentliche Funktionen von Amazon Services zu nutzen, empfehlen wir Ihnen, die Cookie-Funktionen eingeschaltet zu lassen. Wenn Sie Cookies blockieren oder anderweitig nicht akzeptieren, können Sie beispielsweise Waren nicht in Ihren Einkaufswagen legen, zum Checkout gehen oder andere Funktionen von Amazon Services nutzen, die eine Registrierung voraussetzen. Mehr Informationen bezüglich Cookies finden Sie in unseren [Hinweisen zu Cookies](https://www.amazon.de/gp/help/customer/display.html/?nodeId=201890250).
* Wenn Sie unsere Website anonym besuchen wollen, können Sie dies tun, in dem Sie sich von Ihrem Konto [abmelden](https://www.amazon.de/gp/help/customer/display.html?nodeId=GX7AZREFL3D5VC2D) und Cookies in Ihrem Browser deaktivieren.
* Haben Sie in die Verarbeitung Ihrer Informationen für einen bestimmen Zweck eingewilligt, können Sie diese Einwilligung jederzeit widerrufen und wir werden Ihre Informationen für diesen Zweck nicht weiter verarbeiten.
* Sie können sich bei bestimmten anderen Arten der Datenverarbeitung abmelden (Opt-out), indem Sie Ihre Einstellungen auf der entsprechenden Amazon Website (z.B. unter "Meine Inhalte und Geräte"), auf Ihren Geräten oder Apps anpassen. Für mehr Informationen klicken Sie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=GQFYXZHZB2H629WN) . Die meisten Geräte, die nicht von Amazon stammen, gestatten es Nutzern, Erlaubnisse auf dem Gerät zu ändern (z.B. Deaktivierung / Zugriff auf Ortungsdienste, Kontakte). Bei den meisten Geräten sind diese Steuerungen in dem Einstellungsmenü des Gerätes verortet. Falls Sie Fragen dazu haben, wie Sie Berechtigungseinstellungen auf Geräten, die von Dritten hergestellt wurden, ändern, empfehlen wir Ihnen, sich an Ihnen Mobilfunkanbieter oder den Hersteller Ihres Gerätes zu wenden, da verschiedene Geräte verschiedene Berechtigungseinstellungen haben können.
* Verkäufer können bestimmte Informationen in [Seller Central](https://sellercentral.amazon.de/) hinzufügen oder aktualisieren, ihre Kontoinformationen aktualisieren in dem sie auf die [Verkäufer Kontoinformationen](https://sellercentral.amazon.de/hz/sc/account-information) zugreifen und E-Mails und andere Mitteilungen, die sie von uns erhalten anpassen, in dem sie ihre [Benachrichtigungseinstellungen](https://sellercentral.amazon.de/gp/seller/configuration/notificationPreferences.html) anpassen.
* Autoren können Informationen, die sie in dem Autorenportal und auf Author Central bereitgestellt haben, hinzufügen oder aktualisieren, indem sie auf ihr Konto im Autorenportal oder auf Author Central zugreifen.

Zusätzlich haben Sie, innerhalb des jeweils geltenden Rechts, das Recht, Auskunft, Berichtigung und Löschung Ihrer persönlichen Informationen zu verlangen. Weiterhin steht Ihnen das Recht auf Datenübertragbarkeit zu. Sie können unserer Datenverarbeitung widersprechen oder in speziellen Fällen die Beschränkung der Datenverarbeitung von uns verlangen. Möchten Sie eines dieser Rechte wahrnehmen, klicken Sie bitte [hier](https://www.amazon.de/privacy) oder kontaktieren Sie unseren Amazon [Kundenservice](https://www.amazon.de/kontakt).

**Dürfen Kinder Amazon Services benutzen?**

Amazon Europe bietet keine Produkte zum Kauf durch Minderjährige an. Auch unsere Produkte für Kinder können nur von Erwachsenen gekauft werden. Wenn Sie das 18. Lebensjahr noch nicht vollendet haben, dürfen Sie Amazon Services nur zusammen mit einem Elternteil oder Vormund benutzen.

**Wie lange speichern wir Ihre persönlichen Informationen?**

Wir speichern Ihre persönlichen Informationen, um Ihnen die laufende Nutzung der Amazon Services zu ermöglichen. Wir speichern Ihre Informationen solange, wie dies erforderlich ist, um die in dieser Datenschutzerklärung beschriebenen Zwecke zu erfüllen oder wie dies gesetzlich vorgeschrieben wird, z.B. für Steuer- und Buchhaltungszwecke. Andere Speicherdauern werden wir Ihnen mitteilen. Beispielsweise behalten wir Ihre Bestellungsübersichten, damit Sie vergangene Einkäufe und die Adressen, an die Sie Ihre Bestellungen versandt haben, überprüfen können (und falls gewünscht Bestellungen wiederholen können) und damit wir die Relevanz der von uns empfohlenen Produkte und Inhalte verbessern können.

**Kontakte, Hinweise & Änderungen**

Wenn Sie Fragen zum Datenschutz bei Amazon Europe haben oder eine der oben benannten Verantwortlichen Stellen kontaktieren wollen, [teilen Sie uns](https://www.amazon.de/kontakt) bitte eine möglichst genaue Beschreibung Ihres Anliegens mit und wir werden versuchen, Ihr Problem für Sie zu lösen. Darüber hinaus können Sie den Datenschutzbeauftragten der oben genannten datenschutzrechtlichen Verantwortlichen unter **eu-privacy@amazon.de** erreichen. Sie können eine Beschwerde bei unserer federführenden Aufsichtsbehörde, der [Commission Nationale pour la Protection des Données in Luxemburg](https://cnpd.public.lu/de.html) [externer Link], sowie bei einer lokalen Behörde einreichen.

Unser Geschäft ändert sich ständig und genauso ändert sich diese Datenschutzerklärung. Wir empfehlen, regelmäßig unsere Website besuchen und Änderungen zur Kenntnis nehmen. Soweit nichts anderes geregelt ist, unterliegt die Nutzung sämtlicher Informationen, die wir über Sie und Ihre Kundenkonten haben, dieser Datenschutzerklärung. Wir stehen zu den Versprechungen, die wir Ihnen geben und versichern Ihnen, dass wir wesentliche Änderungen unserer Datenschutzerklärung, die zu einem schwächeren Schutz bereits erhaltener Kundendaten führen, stets nur mit der Zustimmung der betroffenen Kunden vornehmen werden.

**Verwandte Themen**

* [Allgemeine Geschäftsbedingungen](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909000)
* [Hilfe-Seiten](https://www.amazon.de/gp/help/customer/display.html?nodeId=508510)
* [Wo ist meine Bestellung?](https://www.amazon.de/gp/help/customer/display.html?nodeId=201910410)
* [Richtlinien für die Teilnahme an der Amazon Community](https://www.amazon.de/gp/help/customer/display.html?nodeId=201929730)

**Beispiele erhobener Informationen**

Sie stellen uns Informationen zur Verfügung, wenn Sie:

1. nach Produkten oder Dienstleistungen suchen;
2. eine Bestellung über Amazon Services aufgeben;
3. Inhalte auf ein Gerät herunterladen, streamen, anzeigen oder verwenden; dies durch ein Service oder eine Anwendung vornehmen oder Apps auf ein Gerät herunterladen oder anwenden;
4. Informationen in [Ihrem Konto](https://www.amazon.de/gp/css/homepage.html/ref=nav_youraccount_btn) (bitte beachten Sie, dass Sie möglicherweise mehr als ein Konto haben, wenn Sie mehr als eine E-Mail-Adresse oder Handynummer beim Einkaufen bei uns verwendet haben) oder in [Ihrem Profil](https://www.amazon.de/gp/help/customer/display.html?nodeId=201929730) angeben;
5. Mit unserem Alexa Sprachdienst sprechen oder anderweitig interagieren;
6. Ihre Kontakte hochladen;
7. Ihre Einstellungen für Ihr Gerät oder einen anderen Amazon-Dienst konfigurieren, hierfür Datenzugriffsrechte zur Verfügung stellen oder mit Ihrem Gerät interagieren;
8. Informationen in Ihrem [Verkäuferkonto](https://sellercentral.amazon.de/) zur Verfügung stellen, oder auch in Ihrem [Kindle Direct Publishing (KDP) Konto](https://kdp.amazon.com/de_DE/), Entwicklerkonto oder in jedem anderen Konto, das wir Ihnen zur Verfügung stellen und das Ihnen erlaubt, Software, Waren oder Dienstleistungen für Amazon-Kunden zu entwickeln oder anzubieten;
9. Ihre Produkte oder Dienstleistungen auf oder über Amazon Services anbieten;
10. Mit uns per Telefon, E-Mail oder anderweitig kommunizieren;
11. Einen Fragebogen, eine Support-Anfrage oder ein Gewinnspiel-Teilnahmebogen ausfüllen;
12. Bilder, Videos oder andere Dateien auf Prime Photos, Amazon Drive oder andere Amazon Services hochladen;
13. Playlisten, Watchlisten, [Wunschlisten](https://www.amazon.de/gp/help/customer/display.html?nodeId=201936660) oder Geschenkverzeichnisse erstellen;
14. An Community-Angeboten teilnehmen; [Kundenbewertungen](https://www.amazon.de/gp/help/customer/display.html?nodeId=201929880) erstellen und bewerten;
15. Eine Terminerinnerung eingeben; oder
16. Den Benachrichtigungsservice für noch nicht erschienene Produkte verwenden, z.B. Nachricht über Produktverfügbarkeit

Durch diese Handlungen können Sie uns folgende Informationen zur Verfügung stellen: Ihr Name; Adresse und Telefonnummer; Zahlungsinformationen; Ihr Alter; Ihre Standortinformationen; Personen, an die Einkäufe versendet wurden oder Personen, die in [1-Click-Einstellungen](https://www.amazon.de/gp/help/customer/display.html?nodeId=201889370) aufgeführt sind (einschließlich Adressen und Telefonnummern); E-Mail-Adressen Ihrer Freunde und anderer Personen; Inhalte von Bewertungen und E-Mails an uns; persönliche Beschreibung und Foto in [Ihrem Profil](https://www.amazon.de/gp/help/customer/display.html?nodeId=201929730); Sprachaufzeichnungen, wenn Sie mit Alexa sprechen; Bilder und Videos, die im Zusammenhang mit Amazon Services gespeichert sind; Informationen und Dokumente bezüglich Identität und Stand; Unternehmens- und Finanzinformationen; Informationen bezüglich Ihrer Kreditgeschichte; MwSt-Nummern; und Geräteprotokolldateien und -konfigurationen, einschließlich W-Lan-Anmeldedaten, wenn Sie diese automatisch mit Ihren anderen Amazon-Geräten synchronisieren lassen.

**Automatische Informationen**

Beispiele für Informationen, die wir sammeln und analysieren, beinhalten:

* Die Internet-Protocol-Adresse (IP), die Ihren Computer und andere Geräte mit dem Internet verbindet;
* Logins, E-Mail-Adressen, Passwörter,
* Informationen über Computer, Geräte und Verbindungen wie z. B. Geräteanwendungen, Browsertypen und -Versionen, Browser-Plugin-Typen und -Version, Betriebssysteme und Zeitzoneneinstellungen;
* Der Standort Ihres Geräts oder Computers;
* Informationen über Content-Interaktionen, wie Content-Downloads, Streams und Wiedergabedetails, einschließlich Dauer und Anzahl gleichzeitiger Streams und Downloads, sowie Netzwerkdetails für Streaming- und Downloadqualität, einschließlich Informationen über Ihren Internetdienstanbieter;
* Geräte Metriken, z.B. wann ein Gerät verwendet wird, Anwendungsnutzung, Verbindungsdaten und alle Fehler oder Ereignisausfälle;
* Amazon Service Metriken (z.B. das Auftreten von technischen Fehlern, Ihre Interaktionen mit Servicefunktionen und -Inhalten, Ihre Einstellungen und Backup-Informationen, Standort Ihres Geräts, auf dem eine Anwendung läuft, Informationen über hochgeladene Bilder und Dateien (z.B. Dateiname, Datum, Uhrzeit und Ort Ihrer Bilder));
* Ihre Bestell- und Inhaltsnutzungshistorie, die wir manchmal mit ähnlichen Informationen anderer Kunden zusammenführen und in nicht persönlich identifizierbarer Form in Features wie Bestseller abbilden;
* Der komplette Uniform Resource Locators (URL) Clickstream zu, durch und aus unserer Website, d. h. die Reihenfolge der Seiten unseres Internet-Angebots, die Sie aufsuchen, einschließlich Datum und Zeit, Cookie- Nummer, der Produkte und/oder Inhalte, die Sie angeschaut oder nach denen Sie gesucht haben, einschließlich der Dauer bis zum Aufbau einer Webseite, deren fehlerhaftes Herunterladen, Informationen zur Interaktion zwischen Seiten (z.B. Scrolling, Klicken, Mouse-overs); oder
* Telefonnummern, die Sie genutzt haben, um den Kundenservice anzurufen.

Auf unserer Website benutzen wir auch Gerätekennungen, Cookies und ähnliche Technologien auf Geräten, Apps und unseren Webseiten, um Browsing-, Nutzungs- und andere Informationen zu erheben. Dies dient zur Vorbeugung vor Missbrauch, insbesondere vor Betrug.

**Informationen aus anderen Quellen**

Beispiele für Informationen, die wir aus anderen Quellen erhalten, beinhalten:

* Aktualisierte Informationen über Bestell- und Lieferadresse von unseren Paketzustellern und anderen Transportunternehmen, die wir dazu verwenden, unsere Datenbank zu aktualisieren, um Ihre nächsten Bestellungen sicher stellen zu können und zu gewährleisten, dass wir mit Ihnen einfacher kommunizieren können;
* Informationen über Konten, Kauf - und Zahlungsverhalten, Page View Informationen, oder andere Informationen über Ihre Interaktionen mit Geschäften, mit denen wir gemeinsam (co-branded) Angebote unterhalten oder für die wir technische, Erfüllungs-, Zahlungs-, Werbe- oder andere Dienstleistungen anbieten;
* Informationen über Ihre Interaktionen mit Produkten und Dienstleistungen unserer Tochtergesellschaften;
* Suchergebnisse und Links, einschließlich bezahlter Listungen;
* Informationen über mit dem Internet verbundene Geräte und Dienste, die Sie mit Alexa verbunden haben; und
* Auskünfte bezüglich der Kreditgeschichte von Kreditauskunfteien, die wir dazu verwenden, Missbrauch, insbesondere Betrug, zu verhindern und aufzudecken und dazu, bestimmten Kunden bestimmte Finanzdienstleistungen und Zahlungsarten anbieten zu können.

**Informationen, zu denen Sie Zugang haben**

Beispiele für Informationen, zu denen Sie bei Amazon Services Zugang haben, sind:

* Status der letzten Bestellungen (einschließlich Abonnements);
* Ihre komplette Bestellungshistorie;
* Persönliche identifizierbare Daten (einschließlich Name, E-Mail-Adresse, Passwort, Kommunikations- und personalisierte Werbungseinstellungen, Adressbuch und 1-Click®-Einstellungen);
* Einstellungen zu Zahlungsarten (einschließlich Bezahlkarteninformationen, Geschenkgutscheinen, Geschenkkarten und Kontoauszüge);
* Angaben darüber, welche Informationen Sie per E-Mail von uns erhalten möchten (einschließlich Verfügbarkeits- und Bestellbenachrichtigungen, Termin-Erinnerungen, Newsletter);
* Empfehlungen und Produkte, die Sie kürzlich angesehen haben und die die Grundlage für Empfehlungen bilden (inkl. Unsere Empfehlungen für Sie und Korrigieren Sie Ihre Empfehlungen);
* Einkaufslisten und Wunschzettel ( einschließlich Wunschlisten und Baby- und Hochzeitsverzeichnisse);
* Ihre Inhalte, Geräte, Dienste und zugehörigen Einstellungen;
* Inhalte, die Sie kürzlich angesehen haben;
* Sprachaufzeichnungen in Verbindung mit Ihrem Konto;
* Der "Mein Profil"-Bereich (einschließlich Rezensionen, Empfehlungen, Erinnerungen, persönliche Profile);
* Verkäufer können ihr Konto und andere Informationen einsehen und ihre Kommunikationseinstellungen anpassen, indem sie ihr Konto in [Seller Central](https://sellercentral.amazon.de/) aktualisieren;
* Autoren können ihr Konto und andere Informationen auf der [KDP](https://kdp.amazon.com/de_DE/)- oder [Author Central-](https://authorcentral.amazon.de/) Webseite einsehen und ihr Konto aktualisieren und
* Entwickler, die an unserem Developer Services Programm teilnehmen, können ihr Konto und andere Informationen einsehen und ihre Kommunikationseinstellungen anpassen, indem sie ihr Konto im [Developer Services Portal](https://developer.amazon.com/) aktualisieren.

**EU-US und Schweiz-US Privacy Shield (EU-US Datenschutzschild)**

Amazon.com, Inc. und bestimmte von ihr beherrschte US-Tochterunternehmen (zusammen die [Amazon-Konzerngesellschaften](https://www.amazon.com/gp/help/customer/display.html?nodeId=202137190), oder "wir") nehmen an dem Programmen EU-US und Schweiz-US Privacy Shield ("EU-US-Datenschutzschild") für die Erhebung, Nutzung und Speicherung von persönlichen Informationen aus Mitgliedsstaaten der Europäischen Union, dem Vereinigten Königreich und der Schweiz teil. Wir haben gegenüber dem U.S. Handelsministerium amtlich bestätigt, die Privacy Shield-Grundsätze einzuhalten. Um mehr über die Privacy Shield-Grundsätze zu erfahren, klicken Sie bitte [hier](https://www.commerce.gov/tags/eu-us-privacy-shield) [externer Link].

Wenn Sie sich über unseren Umgang mit Ihren Informationen unter dem Privacy Shield oder über unsere Datenschutzpraktiken im Übrigen informieren oder beschweren wollen, senden Sie uns bitte eine E-Mail an **privacyshield@amazon.com**. Wir werden Ihre Anfrage umgehend beantworten. Falls wir Ihre Beschwerde im Zusammenhang mit dem Privacy Shield nicht befriedigend beantworten können, oder wir den Eingang Ihrer Beschwerde nicht rechtzeitig bestätigen, können Sie sich an TRUSTe wenden. TRUSTe ist eine unabhängige und unparteiische Schlichtungsstelle mit Sitz in den USA. TRUSTe hat sich verpflichtet, für Sie kostenfrei Beschwerden zu beantworten und angemessene Rechtsmittel zur Verfügung zu stellen. Um mehr über die Dienstleistungen von TRUSTe als Schlichtungsstelle zu erfahren oder um eine Beschwerde an TRUSTe zu richten, klicken Sie [hier](https://feedback-form.truste.com/watchdog/request) [externer Link]. Falls weder Amazon noch TRUSTe Ihrer Beschwerde abhelfen können, können Sie sich für ein verbindliches Schiedsgerichtsverfahren an das Privacy Shield-Panel wenden. Um mehr über das Privacy Shield-Panel zu erfahren, klicken Sie bitte [hier](https://www.commerce.gov/tags/eu-us-privacy-shield) [externer Link].

Wie [hier](https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_2609CB37E82B4A4991D3BECAE70486B7) ausgeführt, geben wir persönliche Informationen manchmal an Dritte weiter, damit diese Aufgaben für uns erfüllen können. Falls wir unter dem Privacy Shield erhaltene persönliche Informationen an Dritte weitergeben, muss der Zugriff, die Nutzung und Offenlegung der persönlichen Informationen durch den Dritten im Einklang mit unseren Verpflichtungen nach dem Privacy Shield stehen, und wir haften unter dem Privacy Shield für die Nichteinhaltung durch den Dritten, es sei denn, dass wir für das Ereignis, das zum Schaden geführt hat, nicht verantwortlich sind.

Sie können unsere Privacy Shield-Registrierung [hier](https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4) [externer Link] einsehen. Die Amazon-Konzerngesellschaften unterliegen den Untersuchungs- und Vollstreckungsbefugnissen der Federal Trade Commission (FTC). Wir können verpflichtet sein, persönliche Informationen, die wir unter dem Privacy Shield verarbeiten, auf rechtmäßige Anforderung durch öffentliche Behörden herauszugeben, einschließlich um Erfordernissen der nationalen Sicherheit oder der Rechtsdurchsetzung zu genügen.

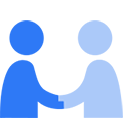
Apple

**Privacy Policy**

**The Apple Privacy Policy was updated on December 31, 2019.**

Your privacy is important to Apple so we’ve developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your personal information.

In addition to this Privacy Policy, we provide data and privacy information imbedded in our products connected with our Data & Privacy Icon for certain features that ask to use your personal information.



You can review this information before enabling these features, in Settings related to those features and/or online at [apple.com/legal/privacy](https://www.apple.com/legal/privacy/). Please take a moment to familiarize yourself with our privacy practices and [contact us](https://www.apple.com/legal/privacy/en-ww/contact/) if you have any questions.  
   
[Your California Privacy Disclosures](https://www.apple.com/legal/privacy/california/)   
[Information Regarding Commercial Electronic Messages in Canada](https://www.apple.com/legal/privacy/en-ww/canada-notice/)  
[Apple Health Research Apps Privacy Policy](https://www.apple.com/legal/privacy/apple-health-studies/en-ww)

**Collection and Use of Personal Information**

Personal information is data that can be used to identify or contact a single person.

You may be asked to provide your personal information anytime you are in contact with [Apple or an Apple affiliated company](https://www.apple.com/legal/privacy/en/affiliated-company/). Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising. You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have.

Here are some examples of the types of personal information Apple may collect and how we may use it:

**What personal information we collect**

* When you create an Apple ID, apply for commercial credit, purchase a product, download a software update, register for a class at an Apple Retail Store, connect to our services, contact us including by social media or participate in an online survey, we may collect a variety of information, including your name, mailing address, phone number, email address, contact preferences, device identifiers, IP address, location information, credit card information and profile information where the contact is via social media.
* When you share your content with family and friends using Apple products, send gift certificates and products, or invite others to participate in Apple services or forums, Apple may collect the information you provide about those people such as name, mailing address, email address, and phone number. Apple will use such information to fulfill your requests, provide the relevant product or service, or for anti-fraud purposes.
* In certain jurisdictions, we may ask for a government issued ID in limited circumstances including when setting up a wireless account and activating your device, for the purpose of extending commercial credit, managing reservations, or as required by law.

**How we use your personal information**

We may process your personal information: for the purposes described in this Privacy Policy, with your consent, for compliance with a legal obligation to which Apple is subject, for the performance of a contract to which you are party, in order to protect your vital interests, or when we have assessed it is necessary for the purposes of the legitimate interests pursued by Apple or a third party to whom it may be necessary to disclose information. If you have questions about this legal basis you can [contact](https://www.apple.com/legal/privacy/contact/) the Data Protection Officer.

* The personal information we collect allows us to keep you posted on Apple’s latest product announcements, software updates, and upcoming events. If you don’t want to be on our mailing list, you can opt-out anytime by [updating your preferences](https://appleid.apple.com/choose-country-region).
* We also use personal information to help us create, develop, operate, deliver, and improve our products, services, content and advertising, and for loss prevention and anti-fraud purposes. We may also use your personal information for account and network security purposes, including in order to protect our services for the benefit of all our users, and pre-screening or scanning uploaded content for potentially illegal content, including child sexual exploitation material. Where we use your information for anti-fraud purposes it arises from the conduct of an online transaction with us. We limit our uses of data for anti-fraud purposes to those which are strictly necessary and within our assessed legitimate interests to protect our customers and our services. For certain online transactions we may also validate the information provided by you with publicly accessible sources.
* We may use your personal information, including date of birth, to verify identity, assist with identification of users, and to determine appropriate services. For example, we may use date of birth to determine the age of Apple ID account holders.
* From time to time, we may use your personal information to send important notices, such as communications about purchases and changes to our terms, conditions, and policies. Because this information is important to your interaction with Apple, you may not opt out of receiving these communications.
* We may also use personal information for internal purposes such as auditing, data analysis, and research to improve Apple’s products, services, and customer communications.
* If you enter into a sweepstake, contest, or similar promotion we may use the information you provide to administer those programs.
* If you apply for a position at Apple or we receive your information in connection with a potential role at Apple, we may use your information to evaluate your candidacy and to contact you. If you are a candidate, you will receive more information about how Apple handles candidate personal information at the time of application.

**Source of your personal information where they are not collected from you**

We may have received your personal information from other persons if that person has shared their content with you using Apple products, sent gift certificates and products, or invited you to participate in Apple services or forums. We may also validate the information provided by you when creating an Apple ID with a third party for security and fraud prevention purposes.

If you are a potential candidate for employment with Apple, we may have received your personal information from third parties such as recruiters or external websites. We will use the personal information we receive to contact you about a potential opportunity or in evaluating your candidacy. If you did not provide us your personal information directly, we will inform you of the source when we first contact you regarding your candidacy. For research and development purposes, we may use datasets such as those that contain images, voices or other data that could be associated with an identifiable person. When acquiring such datasets, we do so in accordance with applicable law in the jurisdiction in which the dataset is hosted. When using such datasets for research and development, we do not attempt to re-identify individuals who may appear therein.

**Collection and Use of Non-Personal Information**

We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

* We may collect information such as occupation, language, zip code, area code, unique device identifier, referrer URL, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.
* We may collect information regarding customer activities on our website, iCloud services, our iTunes Store, App Store, Mac App Store, App Store for Apple TV and iBooks Stores and from our other products and services. This information is aggregated and used to help us provide more useful information to our customers and to understand which parts of our website, products, and services are of most interest. Aggregated data is considered non‑personal information for the purposes of this Privacy Policy.
* We may collect and store details of how you use our services, including search queries. This information may be used to improve the relevancy of results provided by our services. Except in limited instances to ensure quality of our services over the Internet, such information will not be associated with your IP address.
* With your explicit consent, we may collect data about how you use your device and applications in order to help app developers improve their apps.

If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.

**Cookies and Other Technologies**

Apple’s websites, online services, interactive applications, email messages, and advertisements may use ["cookies" and other technologies](https://www.apple.com/legal/privacy/en-ww/cookies/) such as pixel tags and web beacons. These technologies help us better understand user behavior, tell us which parts of our websites people have visited, and facilitate and measure the effectiveness of advertisements and web searches. We treat information collected by cookies and other technologies as non‑personal information. However, to the extent that Internet Protocol (IP) addresses or similar identifiers are considered personal information by local law, we also treat these identifiers as personal information. Similarly, to the extent that non-personal information is combined with personal information, we treat the combined information as personal information for the purposes of this Privacy Policy.

Ads that are delivered by Apple’s advertising platform may appear in Apple News and in the App Store. If you do not wish to receive ads targeted to your interests from Apple's advertising platform, you can choose to enable Limit Ad Tracking, which will opt your Apple ID out of receiving such ads regardless of what device you are using. If you enable Limit Ad Tracking on your mobile device, third-party apps cannot use the Advertising Identifier, a non-personal device identifier, to serve you targeted ads. You may still see ads in the App Store or News based on context like your search query or the channel you are reading. In third-party apps, you may see ads based on other information.

Apple also uses cookies and other technologies to remember personal information when you use our website, online services, and applications. Our goal in these cases is to make your experience with Apple more convenient and personal. For example, knowing your first name lets us welcome you the next time you visit the Apple Online Store. Knowing your country and language − and if you are an educator, your school − helps us provide a customized and more useful shopping experience. Knowing someone using your computer or device has shopped for a certain product or used a particular service helps us make our advertising and email communications more relevant to your interests. And knowing your contact information, hardware identifiers, and information about your computer or device helps us personalize your operating system, set up your iCloud service, and provide you with better customer service.

If you want to disable cookies and you’re using the Safari web browser, go to Safari preferences and then to the privacy pane to manage your preferences. On your Apple mobile device, go to Settings, then Safari, scroll down to the Privacy & Security section, and tap on “Block Cookies” to manage your preferences. For other browsers, check with your provider to find out how to disable cookies. Please note that certain features of the Apple website will not be available once cookies are disabled.

As is true of most internet services, we gather some information automatically and store it in log files. This information includes Internet Protocol (IP) addresses, browser type and language, Internet service provider (ISP), referring and exit websites and applications, operating system, date/time stamp, and clickstream data. We use this information to understand and analyze trends, to administer the site, to learn about user behavior on the site, to improve our product and services, and to gather demographic information about our user base as a whole. Apple may use this information in our marketing and advertising services.

In some of our email messages, we use a “click-through URL” linked to content on the Apple website. When customers click one of these URLs, they pass through a separate web server before arriving at the destination page on our website. We track this click-through data to help us determine interest in particular topics and measure the effectiveness of our customer communications. If you prefer not to be tracked in this way, you should not click text or graphic links in the email messages. Pixel tags enable us to send email messages in a format customers can read, and they tell us whether mail has been opened. We may use this information to reduce or eliminate messages sent to customers.

**Disclosure to Third Parties**

At times Apple may provide third parties with certain personal information to provide or improve our products and services, including to deliver products at your request, or to help Apple market to consumers. When we do, we require those third parties to handle it in accordance with relevant laws. Apple does not sell personal information, and personal information will never be shared with third parties for their marketing purposes. For example, when you purchase and activate your iPhone, you authorize Apple and your carrier to exchange the information you provide during the activation process to carry out service, including information about your device. If you are approved for service, your account will be governed by Apple and your carrier’s respective privacy policies.

**Service Providers**

Apple shares personal information with companies who provide services such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys. These companies are obligated to protect your information and may be located wherever Apple operates.

**Others**

It may be necessary − by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence − for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate. We may also disclose information about you, but only where there is a lawful basis for doing so, if we determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users.  This could include providing information to public or governmental authorities. Additionally, in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party.

**Protection of Personal Information**

Apple takes the security of your personal information very seriously. Apple online services such as the Apple Online Store and iTunes Store protect your personal information during transit using encryption such as Transport Layer Security (TLS). When your personal data is stored by Apple, we use computer systems with limited access housed in facilities using physical security measures. With the exception of iCloud Mail, iCloud data is stored in encrypted form including when we utilize third-party storage.

When you use some Apple products, services, or applications or post on an Apple forum, chat room, or social networking service, the personal information and content you share is visible to other users and can be read, collected, or used by them. You are responsible for the personal information you choose to share or submit in these instances. For example, if you list your name and email address in a forum posting, that information is public. Please take care when using these features.

If you or anyone else using Family Sharing logs on to a device that is owned by a third party, any information shared within your Family—including calendar, location, photos, and iTunes purchases—may be downloaded on to that third-party device thereby disclosing any such shared information. Visit [Family Sharing](https://www.apple.com/icloud/family-sharing/) for more information.

**The Existence of Automated Decision-Making, Including Profiling**

Apple does not take any decisions involving the use of algorithms or profiling that significantly affect you.

**Integrity and Retention of Personal Information**

Apple makes it easy for you to keep your personal information accurate, complete, and up to date. We will retain your personal information for the period necessary to fulfill the purposes outlined in this Privacy Policy and our service specific privacy summaries. When assessing these periods we carefully examine our need to collect personal information at all and if we establish a relevant need we only retain it for the shortest possible period to realize the purpose of collection unless a longer retention period is required by law.

**Your Privacy Rights**

You can help ensure that your contact information and preferences are accurate, complete, and up to date by signing in to your [Apple ID account page](https://appleid.apple.com/choose-country-region). For other personal information we hold, we will provide you with access (including a copy) for any purpose including to request that we correct the data if it is inaccurate or delete the data if Apple is not required to retain it by law or for legitimate business purposes.

We may decline to process requests that are frivolous/vexatious, jeopardize the privacy of others, are extremely impractical, or for which access is not otherwise required by local law. We may also decline aspects of deletion or access requests if we believe doing so would undermine our legitimate use of data for anti-fraud and security purposes as described earlier. Online tools for the exercise of access, deactivation/restriction, correction, or deletion requests are available on a regional basis by signing in to [privacy.apple.com](http://privacy.apple.com/). For users with Shazam accounts sign in to [www.shazam.com/privacy](http://www.shazam.com/privacy). When you make a request using these online tools, we will verify your identity and the legitimacy of your request.

**California**

The California Consumer Privacy Act provides California consumers with the right to obtain from Apple information about the personal information about you that we collect, use, and disclose. You can exercise your rights through an authorized agent by providing relevant details to allow sign in to [privacy.apple.com](http://privacy.apple.com/). If you cannot access Apple’s online tools, you or your agent can make a request to [apple.com/legal/privacy/contact](http://apple.com/legal/privacy/contact) or by calling 1-800-275-2273.

If you choose to exercise your privacy rights, you have the right to not to receive discriminatory treatment or a lesser degree of service from Apple.

**Nevada**

You have the right to opt-out of the sale of your personal information. Apple does not sell your personal information.

See our page on [understanding and controlling your personal information](https://support.apple.com/en-us/HT208501) for more information on exercising your rights. Where the online tool is not currently available for access requests in your region, a request may be made directly to [apple.com/legal/privacy/contact](http://apple.com/legal/privacy/contact).

**Children & Education**

We understand the importance of taking extra precautions to protect the privacy and safety of children using Apple products and services. Children under the age of 13, or equivalent minimum age in the relevant jurisdiction, are not permitted to create their own Apple IDs, unless their parent provided verifiable consent or as part of the child account creation process in Family Sharing or they have obtained a Managed Apple ID account (where available) through their school. For example, a parent must review the [Apple ID and Family Sharing Disclosure](https://www.apple.com/legal/privacy/en-ww/parent-disclosure/) and agree to the [Consent to Apple’s Collection, Use and Disclosure of Your Child’s Information](https://www.apple.com/legal/privacy/en-ww/parent-disclosure/#consent); and the [iTunes Store Terms and Conditions](https://www.apple.com/legal/internet-services/itunes/), before they can begin the Apple ID account creation process for their child. In addition, schools that participate in Apple School Manager and have reviewed and consented to the Managed Apple IDs for Students Disclosure may create Managed Apple IDs for students. The [Managed Apple IDs for Students Disclosure](https://www.apple.com/legal/education/apple-school-manager/) describes how Apple handles student information and supplements Apple’s Privacy Policy. Learn more about [Family Sharing](https://www.apple.com/icloud/family-sharing/), the [Managed Apple IDs](https://www.apple.com/education/it/) and [Restrictions](https://support.apple.com/en-us/HT201304) for children’s accounts. If we learn that we have collected the personal information of a child under 13, or equivalent minimum age depending on jurisdiction, outside the above circumstances we will take steps to delete the information as soon as possible. If at any time a parent needs to access, correct, or delete data associated with their Family Sharing account or child’s Apple ID, they may contact us through one of the options provided at the bottom of this page.

**Location-Based Services**

To provide location-based services on Apple products, Apple and our partners and licensees, such as maps data providers, may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. Where available, location-based services may use GPS, Bluetooth, and your IP Address, along with crowd-sourced Wi-Fi hotspot and cell tower locations, and other technologies to determine your devices’ approximate location. Unless you provide consent, this location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, your device may share its geographic location with application providers when you opt in to their location services.

Some location-based services offered by Apple, such as the “Find My” feature, require your personal information for the feature to work.

**Third‑Party Sites and Services**

Apple websites, products, applications, and services may contain links to third-party websites, products, and services. Our products and services may also use or offer products or services from third parties − for example, a third‑party iPhone app.

Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.

If you purchase a subscription in a third party app or within News, we create a Subscriber ID that is unique to you and the developer or publisher which we use to provide reports to the developer or publisher that include information about the subscription you purchased, and your country of residence. If you cancel all of your subscriptions with a particular developer or publisher, the Subscriber ID will reset after 180 days if you do not resubscribe. This information is provided to developers so that they can understand the performance of their subscriptions.

**International Transfers**

All the information you provide may be transferred or accessed by entities around the world as described in this Privacy Policy. Personal information, relating to Apple services, regarding individuals who reside in a member state of the European Economic Area, the United Kingdom and Switzerland is controlled by Apple Distribution International Limited in Ireland, and processed on its behalf by Apple Inc. Apple uses approved [Model Contractual Clauses](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en) for the international transfer of personal information collected in the European Economic Area and Switzerland. Apple, as a global company, has a number of legal entities in different jurisdictions which are responsible for the personal information which they collect and which is processed on their behalf by Apple Inc. For example, point of sale information in our Retail entities outside the U.S. is controlled by our individual Retail entities in each country. Apple, Online Store and iTunes related personal information may also be controlled by legal entities outside the U.S. as reflected in the terms of each service. Imagery and associated data collected by Apple around the world to improve Apple Maps, and in support of our Look Around feature is transferred to Apple Inc in California.

Apple abides by the [Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules System](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx). The APEC CBPR system provides a framework for organizations to ensure protection of personal information transferred among participating APEC economies. If you have an unresolved privacy or data use concern regarding our APEC CBPR and/or PRP certifications please visit our [third-party dispute resolution provider](https://feedback-form.truste.com/watchdog/request).

**Our Companywide Commitment to Your Privacy**

To make sure your personal information is secure, we communicate our privacy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company.

**Privacy Questions**

If you have any questions or concerns about Apple’s Privacy Policy or data processing, you would like to contact our Data Protection Officer, or if you would like to make a complaint about a possible breach of local privacy laws, please [contact us](https://www.apple.com/legal/privacy/en-ww/contact/). You can always contact us by phone at the relevant [Apple Support](https://support.apple.com/en-us/HT201232) number for your country or region.

When a privacy question or question about personal information received in response to an access/download request is received we have a dedicated team which triages your contact to address your issue. Where your issue may be more substantive in nature, we may request more information from you. All such substantive contacts receive a response within seven (7), days wherever possible - providing a response on the issue raised, requesting additional information where necessary or indicating that a response will require additional time. You may at any time refer your complaint to the relevant regulator in your jurisdiction if you are unsatisfied with a reply received from us. If you ask us, we will endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances.

Where your complaint indicates an improvement could be made in our handling of privacy issues we will take steps to make such an update at the next reasonable opportunity. In the event that a privacy issue has resulted in a negative impact on you or another person we will take steps to address that with you or that other person.

Apple may update its Privacy Policy from time to time. When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy. We will also contact you via your contact information on file, for example by email, notification or some other equivalent method.

Apple Inc. One Apple Park Way, Cupertino, California, USA, 95014

Lichess App

Privacy Policy

Introduction

Lichess.org (“Lichess”) is an online chess site. Users can optionally register for an account; however, certain features are available for registered users only. This is because Lichess needs basic information from its users in order to function. Your information will never be sold or shared to/with third parties, unless required by law.

This privacy policy will detail:  
1. What information Lichess collects;  
2. Why this information is collected and how it’s used;  
3. How cookies are used;  
4. Managing your information;  
5. Storage of the collected information;  
6. Closing your account;  
7. Donations;  
8. Other.

Information Collected

Lichess collects:

1. **User submitted information**.

If you create an account, you will be asked to provide your email address. You can also choose to add content your public user profile.

2. **Technical information**.

If you are a registered user, your IP address and your user-agent linked to your profile. Lichess makes use of “fingerprinting” technology similar to [this](https://github.com/Valve/fingerprintjs2). Furthermore, during a game, Lichess “counts” the number of times the game’s window loses focus (how many times you switch tabs/apps), “blurs”.

3. **Communications**.

Messages and chats are stored by Lichess.

Why this information is collected and how it’s used

1. **User submitted information**.

An email is required when you register for Lichess in order to mitigate multi-accounting. Your email address will remain confidential and is used in case you forget your password. Moderators are able to set email addresses for accounts to assist in troubleshooting.

Any content you add to your profile is optional, and is publicly visible to anyone who visits your profile.

2. **Technical information**.

Your IP address(es) and user-agent(s) are private and are not visible to anybody except to Lichess moderators. This information is used to moderate the website and prevent abuse.

The specific fingerprint information is not visible to any user, including the moderators. Moderators can only see the word “print” in their “mod-zone” (should the user have multiple accounts): it aids moderators to determine if a certain user is creating multiple accounts.

“Blurs” are how many times your game’s window lose focus: i.e.: leaving the game's window once counts as one blur. “Blurs” are only visible to moderators and is one of many factors used in cheat evaluation.

3. **Communications**.

In-game chats and private messages are private. Public chat boxes – such as those in tournaments – are public.

Moderators can view users' communications for moderation purposes, as well as if a user is reported under the reason of “insult”, “troll”, or “other”.

Additionally, users will be reported to the moderators if the system’s “shutup” script auto-report a user for using blacklisted words. [Here](https://github.com/ornicar/lila/blob/8ef4b6e3fe0ea75ec21e28c74fc458e5d7574adc/modules/shutup/src/main/Dictionary.scala) is the “shutup” script’s dictionary and [here](https://github.com/ornicar/lila/tree/8ef4b6e3fe0ea75ec21e28c74fc458e5d7574adc/modules/shutup) is its source.

In both cases, the nine most recent reported user’s inbox messages and private in-game chats will be visible to the moderators.  
  
4. **Disclosing your information**.

Your information will only be disclosed if it is legally necessary to do so. For example, if Lichess is ordered to hand over a certain user’s information, or if someone hacks Lichess.

Cookies

A cookie is a text string that Lichess stores in your browser in order to save your site preferences. An example of this can be your board style and theme you have selected.

Cookies can be cleared at any time from your browser. If you do not want Lichess to store any cookie information, feel free to [disable cookies](http://www.wikihow.com/Disable-Cookies) in your browser, although this may affect your browsing with other websites.

Managing your information

You can edit or delete the information from your profile at any time. If you would like to remove your forum posts and/or Q&A posts, simply message a moderator. Information you delete is deleted from the live site but remains in Lichess’ backups for one year.

Your IP address(es) and user-agent(s) are needed for administrative/moderating purposes and cannot be deleted.

Storage of the collected information

Collected information is stored on Lichess’ servers, which are hosted by OVH. Lichess’ backups create snapshots of the Lichess database at a given date and they can never be modified.

Closing your account

You may choose to close your account at any time, for any reason. You cannot re-open your closed account by yourself; however, moderators are able to open closed accounts. Email contact@lichess.org to ask for your account to be re-opened. Remove the information you shared on your public profile before closing your account, as you will not be able to edit/delete it once your account is closed.

Accounts cannot be deleted because of how an online chess website works: your games are linked to other's games.

Donations

Donations are made through PayPal or by credit/debit card (powered by Stripe). All the proceeds made from the donations go directly into server costs. Should you wish to see how donations are used/how much it costs to run Lichess, you can view a spreadsheet [here](https://docs.google.com/spreadsheets/d/1CGgu-7aNxlZkjLl9l-OlL00fch06xp0Q7eCVDDakYEE/edit).

Other

If you have any questions or concerns regarding this policy, please use the Q&A or email Lichess at contact@lichess.org.

Lichess can change this policy at its discretion.

Yahoo

Privacy Policy

*Yahoo is now part of Oath, a digital and mobile media company with more than 50*[*brands*](https://www.oath.com/our-brands/)*globally, and a member of the*[*Verizon family of companies*](http://www.verizon.com/about/privacy/)*. The way we handle your information hasn’t changed, so Yahoo’s Privacy Policy still governs when you are on a Yahoo site, using a Yahoo app or interacting with our products, services or technologies. We may share non-personal information with our family companies for purposes such as product improvements, research and analysis, and to help them provide you with more relevant experience. We will notify you of any significant changes to the way in which we treat your information by sending a notice to the primary email address specified in your Yahoo account or by placing a prominent notice on our site.*

Welcome to the Yahoo Privacy Centre—take a look around. You'll learn how Yahoo treats your personal information, along with ways to control your preferences and settings. As always, Yahoo is committed to gaining your trust.

**What This Privacy Policy Covers**

**Yahoo takes your privacy seriously. Please read the following to learn more about our privacy policy.**

**How Yahoo Uses Your Personal Information**

This policy covers how Yahoo treats personal information that Yahoo collects and receives, including information related to your past use of Yahoo products and services. Personal information is information about you that is personally identifiable like your name, address, email address, or phone number, and that is not otherwise publicly available.

**This privacy policy only applies to Yahoo**

This policy does not apply to the practices of companies that Yahoo does not own or control, or to people that Yahoo does not employ or manage. In addition, some companies that Yahoo has acquired have their own, preexisting privacy policies which may be viewed on our [acquired companies page](https://policies.yahoo.com/in/en/yahoo/privacy/topics/acquiredcompanies/index.htm).

**Information Collection And Use**

**General**

Yahoo collects personal information when you register with Yahoo, when you use [Yahoo products or services](https://policies.yahoo.com/in/en/yahoo/privacy/products/index.html), when you visit Yahoo pages or the pages of certain Yahoo partners, and when you enter [promotions or sweepstakes](https://policies.yahoo.com/in/en/yahoo/privacy/products/promotions/index.htm). Yahoo may combine information about you that we have with information we obtain from business partners or other companies.

When you register we ask for information such as your name, email address, birth date, gender, postal code, occupation, industry, and personal interests. For some financial products and services, if offered, we might also ask for your address and information about your assets. When you register with Yahoo and sign in to our services, you are not anonymous to us.

Yahoo collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services if they are offered.

Yahoo automatically receives and records information from your computer and browser, including your [IP address](https://policies.yahoo.com/in/en/yahoo/privacy/topics/ipaddress/index.htm), Yahoo [cookie](https://policies.yahoo.com/in/en/yahoo/privacy/topics/cookies/index.htm) information, software and hardware attributes, and the page you request.

In addition, when you use Yahoo's services, you may choose to make some of your personal information public. If you post personal information online that is accessible to the public, you may receive unsolicited messages from other parties in return and Yahoo will not be responsible for the use or misuse of such information.

Yahoo uses information for the following general purposes: to customise the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients. Yahoo is not responsible for the accuracy, completeness, veracity nor reliability of any advertising and content, products or services which may be accessed or advertised to you and Yahoo will not be liable for any loss or damage arising out of the same.

**Children**

Yahoo does not contact individuals under age 13 about special offers or for marketing purposes without an adult's permission.

Yahoo does not ask an individual under age 13 for more personal information, as a condition of participation, than is reasonably necessary to participate in a given activity or promotion.

**Information Sharing And Disclosure**

Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

* We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.
* We have a parent's permission to share the information if the user is an individual under age 13. Parents have the option of allowing Yahoo to collect and use their child's information without consenting to Yahoo sharing of this information with people and companies who may use this information for their own purposes.
* We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.
* We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.
* We transfer information about you if Yahoo is acquired by or merged with another company. In this event, Yahoo will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women ages 18-24 from a particular geographic area.

* Yahoo does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
* Yahoo advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

Yahoo works with vendors, partners, advertisers, and other service providers in different industries and categories of business. For more information regarding providers of products or services that you've requested please read our detailed [reference links](https://policies.yahoo.com/in/en/yahoo/privacy/topics/thirdparties/index.htm).

**Cookies**

Yahoo may set and access Yahoo [cookies](https://policies.yahoo.com/in/en/yahoo/privacy/topics/cookies/index.htm) on your computer.

Yahoo lets [other companies](https://policies.yahoo.com/in/en/yahoo/privacy/topics/thirdparties/index.html) that show advertisements on some of our pages set and access their cookies on your computer. Other companies' use of their cookies is subject to their own privacy policies, not this one. Advertisers or other companies do not have access to Yahoo's cookies.

Yahoo uses [web beacons](https://policies.yahoo.com/in/en/yahoo/privacy/topics/webbeacons/index.htm) to access Yahoo cookies inside and outside our network of web sites and in connection with Yahoo products and services.

**Your Ability to Edit and Delete Your Account Information and Preferences**

**General**

You can edit your [Yahoo Account Information](http://edit.yahoo.com/config/eval_profile), including your [marketing preferences](https://subs.communications.yahoo.com/unsubscribe_all.html?c=1111?), at any time.

New categories of marketing communications might be added to the Marketing Preferences page from time to time. Users who visit this page can opt out of receiving future marketing communications from these new categories or they can unsubscribe by following instructions contained in the messages they receive.

We reserve the right to send you certain communications relating to the Yahoo service, such as service announcements, administrative messages and the Yahoo Newsletter, that are considered part of your Yahoo account, without offering you the opportunity to opt out of receiving them.

You can delete your Yahoo account by visiting our [Account Deletion](https://edit.yahoo.com/config/delete_user) page. Please [click here](https://policies.yahoo.com/in/en/yahoo/privacy/topics/datastorage/index.htm) to read about information that might possibly remain in our archived records after your account has been deleted.

**Children**

Parents can review, edit, and delete information relating to their child's Yahoo account using tools offered by [Yahoo Family Accounts](https://safety.yahoo.com/).

If a parent chooses not to allow us to further collect or use a child's information, parents enrolled in Yahoo Family Accounts can delete their child's account by signing into that child's account and then visiting our [Account Deletion](https://edit.yahoo.com/config/delete_user) page. Please [click here](https://policies.yahoo.com/in/en/yahoo/privacy/topics/datastorage/index.htm) to read about information that might possibly remain in our archived records after your account has been deleted.

**Confidentiality And Security**

We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.

We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.

To learn more about security, including the security steps we have taken and security steps you can take, please read [Security at Yahoo](https://policies.yahoo.com/in/en/yahoo/privacy/topics/security/index.htm).

**Changes To This Privacy Policy**

Yahoo may update this policy. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address specified in your Yahoo account or by placing a prominent notice on our site.

**Questions And Suggestions**

If you have questions or suggestions, please complete a [feedback form](https://io.help.yahoo.com/contact/index?page=contactform&locale=en_TH&token=Zh%2FBBVqXzLHlIbokbUqVWTUbuuQeXGkGnZzhKR2JQ4O6mMQdy9JSWfJCJWvc4C3%2F4ml2UKrHQ0nko7rLtSR524MJxCBJKi0QupzNgfCBznvn27xUEp0LLP5v6N84OyIWfjF0v%2BzoPso6e%2F64KJ%2FpFyU2mT99MquR&selectedChannel=email-icon) or you can contact us at:

Yahoo India Private Limited

(CIN: U72900MH2000PTC138698)  
Unit No. 304, 3rd Floor  
Satellite Gazebo, East Wing  
Guru Hargovindji Marg, (A G Link Road)  
Andheri (East), Mumbai – 400093, India  
Phone: +91 22 3308 9600  
Fax: +91 22 3308 9700

*Last updated: 13 June 2017*

Spiegel Online Newspaper

Dear Reader,

How do we analyze your activity on our websites? Which advertising is presented to you? How can you view your personal data if you are a digital subscriber or registered user? In short, how do we deal with the data that arises from the users of our digital products and services? We aim to answer these and many other questions in this data protection declaration.

The regulations for data collection, processing and usage defined here apply as soon as you use one of our digital products or services, set up a user account or navigate one of our sites in any other way. They define the basis for data protection on our sites. Important: For some actions we work with selected partners - on service pages, for example, or when you buy products, for competitions, in the analysis of usage of our content, products and services as well as the integration of advertising. In these cases, you may find additional references to the data protection regulations of these partners. If the content of third parties – particularly of social networks and platforms – is integrated, this may also contain data; this will be explained at greater length later on. You may opt out of any analysis or services that are not essential for the operation of the products and services we offer. We will also explain how to do this.

**1 | The essentials in brief**

Before we begin, though: There are two ways of using our products and services. With our "PUR” option, we dispense entirely with advertising tracking and also, to the greatest extent possible, with advertising.

If you want to continue reading this site for free, however, we cover the costs, with your consent, with further advertising and, in particular, with advertising tracking to serve and optimize those ads. In order to facilitate this, we store and use cookies, device IDs and similar tracking technologies on end devices. The legal basis for this is the European Cookie or ePrivacy Directive in conjunction with the German Telemedia Act (Telemediengesetz; Par 12 et seq.) and/or the European General Data Protection Regulation (Art. 6, Par 1, lit. f (legitimate interest). We have provided an overview of the advertising service providers approved for use in our free content offerings [here](https://spiegel.media/technik/trackingrichtlinienneu). You may revoke your consent to advertising tracking at any time. Should you do so, however, the only way for you to continue to receive unrestricted access to the site is by selecting the "PUR” option.

Delete cookies:

Alle Cookies löschen

In both cases, "business-critical” cookies and tracking technologies are used regardless of consent. These include analysis tools and services for measuring reach, including SZMnG (next generation scalable central measuring procedures) from [INFOnline GmbH](https://www.infonline.de/) and services provided by the German Audit Bureau of Circulation ([IVW](http://www.ivw.eu/)) or the German Association of Online Research ([AGOF](http://www.agof.de/)). We also collect data necessary for ensuring the constant security and functionality of our websites. A more detailed overview of these services and cookies and the options available for partial opt outs (i.e. deactivating tracking) can be found in Section 4. The legal basis for this is also the European Cookie or ePrivacy Directive in conjunction with the German Telemedia Act (Telemediengesetz; Par 12 et seq.) and/or the European General Data Protection Regulation (Art. 6, Par 1, lit. a (consent) and f (legitimate interest).

We recommend the PUR option if you wish to deactivate advertising- or third-party tracking on our website. Simply activating the Do Not Track Mode in your browser is not sufficient. As an alternative, you have the possibility of individually "opting out” of all the service providers that are listed.

The deactivated services are not only blocked for our services, but also generally for the device that you are using. The settings are saved for your device or browser. If you are using more than one browser on more than one device, you must (de-)activate settings on each browser individually, because we are neither able nor permitted to synchronize opt-outs for you. The "PUR” option with log-in, on the other hand, is of course active on all devices.

The list of cookies and services that are used changes from time to time, so please visit this page on a regular basis. We update the information frequently and always in compliance with the legal framework.

However, this in no way affects your fundamental right to data protection. Should we hold personal data about you, you have the right to information and rectification at any time, and in most cases to restriction of processing, erasure, blocking and/or transfer of the data to you. Details about these rights are provided in Section 10. If you have any questions, you can contact us at any time at [datenschutz@spiegelgruppe.de](mailto:datenschutz@spiegelgruppe.de).

**2 | What we promise you**

We will store, process and use your data only in the manner described in this notice, and in compliance with German and European data protection legislation. Naturally, we maintain data secrecy. We treat your data confidentially and do not pass it on to third parties other than to closely associated service providers, who may process subscriptions, payment services, video delivery, or premium and advertising business or other services on our behalf. These service providers are under obligation to use your data only for the purpose provided for in the relevant contract, and not to pass it on to anyone else under any circumstances. When we refer to "we" in this declaration, this also includes these closely associated service providers.

Only when you are registered and logged in with us will your user account – including concrete details about you – be stored in certain cookies, so that you can use our products and services without having to log in every time. All other data collected by way of cookies, device IDs or similar procedures is used pseudonymously and they are not merged with the customer or profile data stored by us. For additional information about advertising tracking, third-party cookies and our analysis of activity on our website, please see Section 1. This data, however, is only used to a limited extent for the personalization of our website, for advertising and for market research, provided you have given[your express consent](https://www.spiegel.de/extra/a-1207772.html), which can be done in each individual case.

Whenever you visit our websites, we temporarily store the IP address of your Internet access and the pages you call up, or in the apps, the device number, if applicable, so that basic services such as authorization assignment can function. However, we never identify you personally with this data and we always delete this data after 30days.

The latest SSL security standard (256-bit Secure Socket Layers) is used across all of our products and services. Your data is encrypted directly during transmission and all data protection-relevant information such as credit card number, bank code, bank account number, name and address is stored in encrypted form in a protected database. In order to administer your shopping cart, we need a session cookie (which is deleted when the browser is closed) or, alternatively, a session identifier in the access path of the web pages (12 digits preceded by a dollar sign) that is invalidated after a half hour of inactivity (the shopping cart and data are then discarded).

**3 | What we know about you as an individual**

* We can only recognize you by your name, your address, your age and other personal details if you have supplied them yourself -- either to us, or perhaps to our implementation partner Plenigo, which is closely integrated into our site and manages digital subscriptions, and which is obliged to protect your data that they process on our behalf -- when, for example, registering for a digital subscription, for the use of our forums or to take advantage of other parts of the website by way of a user account. Data protection information pertaining to classic print subscriptions to DER SPIEGEL can be found [here](https://www.spiegel.de/extra/der-spiegel-abo-allgemeine-geschaefts-und-lieferbedingungen-a-1211959.html).
* We only know you by your email address if you have used it to directly register with us for a newsletter, forum or a contest, for example, or with one of our cooperation partners such as Newsletter2Go, MailChimp or Salesforce, which send emails on our behalf and which also must protect your data in the framework of our cooperation. In the event of contests, we may pass your data on to prize sponsors for processing -- to send the prize, for example, within the scope of the applicable conditions for participation for each contest.
* We only know you by your mobile phone number if you have actually registered it for a digital service, such as our headline news in WhatsApp or Telegram operated by our partner WhatsBroadcast, which offers a service on our behalf and as a processor must also protect your data. For information about the use of data relating to classic print subscriptions, we refer you to this [data protection information](https://www.spiegel.de/extra/der-spiegel-abo-allgemeine-geschaefts-und-lieferbedingungen-a-1211959.html).

In each case, we process your data on the basis of your consent and then only use the respective data in the provision of the actual products and services for which you have registered. If you contact us as an identifiable individual, through a contact form, for example, in addition to your name and email address we may also store such details in our system as the time and place a registration takes place or a message is sent to us; the download, purchase or attempted purchase of products or services; in some cases, also the dispatch or opening of newsletters, emails and push messages; also contact via email or interest in individual products or services. As long as and to the extent that we do not need to make the data available due to legal or contractual requirements, you may revoke your consent for usage at any time. This often requires nothing more than unsubscribing from the product or service in question, but naturally this means that you can no longer use it. You can always find more information on unsubscribing directly in the product or service in question. For newsletters, you can unsubscribe directly in the newsletter itself, from the WhatsApp service in WhatsApp, and so on.

Essentially, we only process personal data to fulfill our contractual obligations to our users. We need to process data to be able to, for instance, suggest suitable products and services or information to you. With certain products and services, we have to ensure that access requests come from humans and not automated programs. To prevent such abuses, we use Google's reCaptcha service, which uses a truncated version of your IP address and other necessary data (only in the event of technical outage in Europe, for instance, is it possible that the IP address will be truncated in the USA). The reCaptcha data is not merged with other Google data.

Please note that if you make a purchase through one of our apps, the payment is usually processed by Apple or Google as the operator of the respective app store. The companies receive your order information and link it to your App Store account to complete the purchase transaction and inform us of your eligibility to access paid products like subscriptions. Under no circumstances, however, do we receive your personal profile and payment data from the stores in question – that is the responsibility of the respective app store operators.

**4 | How we analyze the usage of our products and services**

Which articles are currently being read? How often? By how many people? How much time do viewers spend watching videos? How often do users visit our sites? For us it is important to learn about the preferences and desires of our readers. That's why we use analysis services which can offer us trending topics in real time and comparison with the competition on a daily or monthly basis. The legal basis for this is the European Cookie or ePrivacy Directive in conjunction with the German Telemedia Act (Telemediengesetz; Par 12 et seq.) and/or the European General Data Protection Regulation (Art. 6, Par 1, lit. a (consent) and f (legitimate interest). These services are largely integrated via the Google Tag Manager, which does not collect any data itself. We also never record you as an individual -- at most we use a pseudonym and we do not present advertising or other products or services on the basis of that information.

Instead, for as long as, and to the extent that you have not decided to obtain a "PUR" subscription, advertising trackers are used, about which you can find further information [here](https://www.spiegel.de/services/spiegel-media-datenschutz-tracking-cookies-dsgvo-trackingrichtlinien-und-privacy-a-147b9046-fa1b-4b7b-b5fa-a66114ffacea?d=1590678250).

Irrespective of the consent to advertising tracking, the PUR service also uses "business critical" cookies and tracking technologies, for reach measurement and function assurance in particular. You can find additional information about those cookies here in tabular form, with the names of the respective cookies / tracking services and their attributes.

In addition, the following general information applies:

* Market reach comparison: The aim of the reach measurement is to determine the intensity of use, the number of users of a website and their surfing behavior statistically – i.e. on the basis of standard procedures that are applied in a uniform manner – and to thus obtain comparable values across the market. The company [INFOnline](https://www.infonline.de/) analyzes the general reach of our sites and other sites in Germany with anonymized cookies and/or information that your browser automatically transfers – you can find details on anonymization at the end of this declaration. The data is used for official reach comparison by the associations IVW (www.ivw.eu), AGOF (www.agof.de) and agma (www.agma-mmc.de). You can opt out of this measuring in web browsers [here](https://optout.ioam.de/) ; in apps you can deactivate them in settings (for iOS in iOS Settings > App > AGOF-Zählung, for Android directly in the app menu under Data protection > IVW/AGOF-Zählung). Through the company [INFOnline](https://www.infonline.de/) , we also set session cookies from the copyright collective VG Wort, which analyze the use of a specific text without recording your data, not even anonymously. The analysis is performed to estimate how often texts are printed, copied or otherwise reproduced. Authors are then paid a share of the copyright fees to which they are legally entitled. You can also object to the session cookies of VG Wort using the links mentioned above.
* General analysis with Adobe Analytics: To comprehensively optimize our products and services, we use the web analysis service from Adobe, which uses cookies to scan the usage of our websites both in real time and over the long term. The information collected, including your IP address, is transmitted to the service's servers in Europe, where it is anonymized, (replaced by a generic string of characters) and stored. We use this information to evaluate user activity on our website, to compile reports on website activity and to offer personalized services relating to website and internet use. Because of the anonymization process, no personal or pseudonymous data is stored. You can block cookies, and thus also prevent Adobe analytics, by changing your browser settings. Assistance in doing so can be found [here](https://www.adobe.com/privacy/opt-out.html).
* General analysis with Google Analytics and supplementary services: To comprehensively optimize our products and services beyond this analysis, in a few stand-alone areas of the site such as abo.spiegel.de, we use the web analysis service Google Analytics, which uses cookies to scan usage both in real time and over the long term. The data is generally transferred to U.S. servers and stored there; however, because we have activated IP anonymization, Google must first truncate your IP address in an EU or EEA country (only in the event of technical outage in Europe, for instance, is the IP address first truncated in the U.S.). Even when you have registered with us through a user account and are logged in, you will never be personally identified in Google Analytics – rather only through a pseudonym that we create from your user account and for which organizational measures prevent any connection to you. In particular, we need this pseudonym to standardize analytics data from your various devices and browsers and to optimize our products and services across them. To learn more about the basic composition of our users – even if many readers are not registered – we also use the AMP Client ID interface to integrate text usage with the rapid AMP standard for mobile devices; we also use Google Advertising Reporting Features to interweave anonymous usage data with demographic and interest data from Google’s DoubleClick advertiser network and the Google advertising services that we use. You can find out more about deactivating cookies from DoubleClick (with whom we share anonymous usage data) in the section on our advertising partners. In each case, Google works on our behalf and guarantees not to merge data from Analytics with other Google data. You can reject the above-mentioned data capture and processing in web browsers [here](http://tools.google.com/dlpage/gaoptout?hl=de) by installing a browser plug-in; in apps you can deactivate it in settings (for iOS in iOS Settings > App > Google Analytics, for Android directly in the app menu under Data protection > Google Analytics).
* Optimization analysis with Google Optimize and Hotjar: We use the analysis service Google Optimize to experimentally configure our sites in a number of different variations and to optimize them using comparative statistics. By using cookies, we can anonymously differentiate between test groups. The data is processed by Google Analytics in the manner described; if you deactivate Google Analytics, your data is not included in the comparative tests. We also use spot samples to analyze movement, clicks or swiping behavior on some of our webpages to improve the structure of our products, services and pages. For this purpose, the European service Hotjar records random and anonymized data during a small share of sessions. As such, it is impossible to identify any individual. This data is stored anonymously in Ireland and deleted after a maximum of 365 days. It can be deleted earlier upon request.
* Usage analysis with Firebase and Pushwoosh: We use the services Firebase and Pushwoosh to bring information into websites and apps in real time, for example push messages in apps. These are integral components of our products and services and cannot be deactivated. Anonymous data is also sent to Firebase and Pushwoosh so that we too may analyze usage.
* App analysis with Localytics: To better understand the usage of our apps for smartphones and tablets, we perform analysis in some apps using the service Localytics – how often they are accessed, what is clicked on, etc. Your data is pseudonymized and you are never identified as an individual. You can deactivate the analysis in settings (for iOS in iOS Settings > App > Deactivate sending of usage data; in Android directly in the app menu under Settings).
* Newsletter statistics: We track clicks from our newsletters to our products and services with the help of the statistics services mentioned, and we also analyze opening and click rates as well as other usage data for individual newsletters with our service providers Newsletter2Go, MailChimp and Salesforce. Your email address is stored in a recipients list used to maintain distributions and sometimes also used in pseudonymized form to send you personalized newsletters tailored to your preferences. You can unsubscribe from the newsletter at any time.
* Market research: In surveys, we may sometimes ask for details on usage of our products and services and for demographic details such as age and sex. Your responses are collected anonymously and separately from other data, meaning no connection can be made to you as an individual. We need this for our own, legally permissible analysis and to present proposals to potential partners, advertising customers and other contacts. Data from accompanying betting games for which you may have submitted your email address, for instance, is recorded separately and not associated with your responses.
* Typeform and CognitoForms: We use these tools in some products and services to present surveys and forms on our pages to enable you to provide us with feedback or send us messages, for example. The data is also stored on servers in the U.S., but it is treated confidentially and only evaluated by a limited group of people in our company. You can find out more about data protection at [Typeform](https://admin.typeform.com/to/dwk6gt) and[CognitoForms here](https://www.cognitoforms.com/privacy).

**5 | What social networks and external tools can see about you through us**

On our site, we integrate posts and recommendation functions from platforms such as Facebook, YouTube, Twitter, Instagram, Giphy, Imgur, Spotify, TikTok or the mapping service Mapbox. These services are inactive by default, but they can be activated by the user. Most of these services are based in the U.S. but are nonetheless subject to the applicable data protection regulations in EU and EEA countries. If, for instance, you actively use a recommendation bar on our site or read an article with an embedded post or YouTube video or Spotify playlist, the embedding technology may transfer general framework data such as your IP address back to the social networks and platforms. We have no influence over the way these platforms use the data, including, in some cases, the creation of user profiles. Please consult Facebook, Twitter, Spotify, TikTok and YouTube, among others, directly for more information, and to adjust your privacy settings.

For social networks and on other external platforms, the companies' respective data protection regulations apply, even if we distribute information and maintain presences there with our brands. With Snapchat, in particular, we are active outside our internet presence, for example with DER SPIEGEL in the network’s Discover section. The U.S. company provides us with its content management system and general usage data, such as the number of hits, the length of usage, the demographics of readers and the usernames of all contacts. You can read the network's data protection rules[here](https://www.snap.com/de-DE/privacy/privacy-policy/).

You can also create a user account with us by connecting to your Facebook account ("Sign in with Facebook” function). In this case, of course, we will not have access to your Facebook log-in information -- the social network's privacy policy applies -- but we will need to obtain your public information and your email address in order to allow you to register with us. This will enable you to set up a user account with us, and you can later unlink Facebook in our login area at any time in order to log in to us independently of Facebook.

**6 | How advertising works in our products and services**

If you have not decided to take advantage of the paid "PUR" service, advertisements will be served to cover the costs of our products and services. In online advertising, advertisers need reliable information about how many readers view their ads. Moreover, they are interested in preferentially presenting their advertising to those who are likely to be interested in certain products or topics. To enable them to do so, we allow our advertising partners on our free products and services to track usage data for "usage-based" online advertising (in which advertising is tailored to the user's interests), in other words to collect and process it in usage profiles in pseudonymized form ("Ad tracking”). This data helps ensure that you are presented with advertising to which you are likely to be more attentive. You can identify this "advertising tracking" by the OBA symbol, a turquoise triangle with an "i" in the middle. We have explained how you can deactivate tracking by advertising partners and the legal basis that applies at the very beginning of this data protection statement in Section 1.

We have provided an overview of the advertising service providers, the so-called "Third-Party Trackers” approved for use on our free content offerings [here](https://www.spiegel.de/services/spiegel-media-datenschutz-tracking-cookies-dsgvo-trackingrichtlinien-und-privacy-a-147b9046-fa1b-4b7b-b5fa-a66114ffacea?d=1590678250). The following advertising partners, which also use tracking options, perform particular functions on our site. In some cases, you may need to unsubscribe from them separately:

* IP Deutschland is jointly responsible with us for data processing in the marketing of our website. To serve personalized advertising based on a person's individual interests and to reach target groups, the company measures reaches, controls the delivery of ads, limits them with so-called frequency capping and employs cookies and other identification options to analyze your clicks. Other sources are also used, including, for example, profile segments from registration areas, device data, behavior patterns in our products and services, at times sociodemographic data or assumptions about them. This also extends beyond our website, but it is always in the form of pseudonymized profiles in which you are never directly identified as an individual. Your data will also only be used for relatively short periods of time. You can find detailed information about the technology, the data used, service providers and participants employed, options for opting out, the storage duration and more [here](https://datenschutz.ip.de/nutzungsbasierte_onlinewerbung/informationen_externe_vermarkt.cfm). You can also find all the details about our partnership with IP Deutschland at the end of this data protection statement.
* In addition to the usage analysis with the analytics cookies described above, Google is also integrated as an advertising partner through Google AdWords and can place and use advertising cookies with us according to the same guidelines. If you click on an ad placed by Google, a cookie is stored without personal data that is valid for 30 days and registers your clicks on the ad on our website and is used for statistics. You can opt out [here](http://www.google.com/settings/ads/onweb/?hl=d).
* Outbrain presents both individualized advertisements and personal reading recommendations from our products and services at the bottom of articles. The data that appears there is not actually compiled by us, rather it is used solely by the British service provider, which is subject to EU and EEA regulations. To deactivate Outbrain, click [here](https://www.outbrain.com/legal/privacy#advertising_behavioral_targeting) and scroll down to "Opt-out."
* Sparwelt presents voucher deals on article and overview pages in our products and services; this is subject to additional data privacy regulations, which you can find [here](https://gutscheine.spiegel.de/datenschutz).

In general, Tracking means that your usage of our products and services is captured, for instance individual clicks, subpages visited, advertising banners viewed, etc. Because such data is related to you as a person, all usage data is saved with a random pseudonym, and this pseudonymous data cannot be personalized again. To enable ads to be tailored to your needs in places where cookies do not work optimally, in apps on smartphones, for example, cookie-like technologies may be used. To prevent this, go to the app "Google Settings" on Android smartphones or scroll down to "Google" in the General Settings app, tap "Ads Settings" and tap the on-off slider next to "Personalized advertising." On iOS devices, for which we use Apple's Advertising Identifier, go to the Settings app, then to "Privacy," then to "Advertising" and make your specific settings.

Finally, we use a service from Sourcepoint to prevent the use of ad blockers on our site. This stores data on usage of our site in cookies to repel advertising blockers and record your settings. All analysis is carried out anonymously and not in a personalized way. Private data such as IP addresses are used only in truncated form.

**7 | What our editorial cooperation partners analyze**

In our articles, we often use services from cooperation partners, for surveys or discussion questions, for instance. As with social networks and platforms, the following applies: If, as an example, you read an article with an embedded survey, theoretically general framework data such as your IP address may be transferred back to the social networks and platforms. You can also find more information on their data protection policies on the websites of the cooperation partners:

* **Civey:** In some products and services, we use this German platform to carry out opinion surveys. Civey also collects data on your personal settings and your voting behavior, which is why you can only fully utilize the service once you log in with your own log-in or through Facebook (in the latter case the social network may theoretically track the fact that you use Civey). If you are not logged in, your voting behavior will be evaluated in anonymized form and a cookie set in each case. Your log-in and voting data is stored in encrypted form on German servers, where it remains confidential and is used solely for survey purposes. You can find out more about data protection details for Civey [here](https://civey.com/datenschutz).
* **Opinary:** In some products and services we use this German platform to carry out rapid opinion surveys. Only when you register there are you identifiable as an individual, otherwise a cookie will be set in order to present you with usage-related advertisements; Opinary analyzes the usage of websites and advertising space where it is deployed. You will only be captured using a pseudonym. You can opt out [here](https://compass.pressekompass.net/static/optout.html).
* **Playbuzz:** In some products and services we use this Israeli platform to present our quizzes and other games and interactive surveys. Playbuzz may set cookies for advertising purposes. This is impeded if you deactivate the use of advertisement cookies in your browsers; your browser and device may be roughly identifiable through characteristics such as operating system and other settings. You can find more data protection details for Playbuzz [here](http://www.playbuzz.com/PrivacyPolicy). We have neither influence on their data processing nor are we aware of the full extent of the data collection, the purposes or storage periods.
* **Datawrapper:** We use this service to create editorial information graphics to accompany our articles. When you load these infographics, general usage data is recorded, but not the IP address of your device. In addition, Datawrapper will not pass on any user data to commercial third parties. You can find more about data protection at Datawrapper [here](https://www.datawrapper.de/privacy/).
* **Games:** Some of our products and services include embedded browser-based games that are provided by our Karlsruhe-based partner kr3m, which stores the log files of the websites and files that are accessed, the associated time data, the browser and operating system and the IP address including the provider. This data is used solely for statistical purposes to optimize security and the product or service itself, but also to track illegal use. In no case is personal data passed on without the user's consent. You can find more about data protection at kr3m [here](https://kr3m.com/datenschutz).

**8 | How we advertise ourselves**

We, too, advertise our products and services on the Internet. We use various options for individualized advertisements with which we aim to reach you and other potential readers directly:

* **Google Remarketing:** We use Google's Remarketing function to present you with advertisements for our products and services that correspond with your usage preferences in the global Google advertising network. You will be identified in this network through cookies, but not identified as an individual. You can opt out [here](http://www.google.com/settings/ads) .
* **Facebook Remarketing/Retargeting:** We have integrated remarketing tags from the social network in our products and services where appropriate. If you are logged into Facebook, the platform receives the information that you have visited our site, through which we can present you with advertising on Facebook. The transfer of your data as a Facebook user is regulated in the data protection declaration of the network itself. You can deactivate the "custom audiences" setting for your profile [here](https://www.facebook.com/settings/?tab=ads) . We do not use the custom audience e-mail procedure.
* **Bing Ads:** This service from Microsoft, a U.S.-based company, sets a cookie if you access our website through a Bing ad so that we can find out the total number of clicks leading from an ad to our website. Your user profile is only stored in a pseudonymized form. You can opt out [here](http://choice.microsoft.com/de-DE/opt-out) .
* **Sovendus:** This German service provider offers some of our products for sale on the Internet as an advertising partner. In order to ensure correct billing, the service sets a single pixel at the time of purchase in order to transmit the ordered product in a pseudonymized and encrypted form, including time stamp and IP address, whereby the latter is only used for data security purposes and is normally anonymized after seven days. Details on data protection at Sovendus can be found [here](https://www.sovendus.de/de/datenschutz/).

**9 | Also good to know**

The responsible authority for data processing is the company within the SPIEGEL Group named in the respective legal notice (Impressum), represented by its management. You can always contact the SPIEGEL Group, Kennwort Datenschutz, Ericusspitze 1, 20459 Hamburg or send an email to [datenschutz@spiegelgruppe.de](mailto:datenschutz@spiegelgruppe.de) if you have questions about the way we collect, process or use your data; if you wish to rectify, delete or block such data; or if you have any other general questions that have not been answered. You can find more detailed information about your rights in Section 11. You can also contact the Data Protection Officer for the SPIEGEL Group in this way. We will always address your concern promptly as long as we are not legally prevented from doing so. If we do not address your concern within the legal time limit or fail to address it sufficiently, you may lodge a complaint with the responsible supervisory authority. Generally speaking, the authority applicable to the headquarters of the company is responsible, so for us this is the [Hamburgische Beauftragte für Datenschutz und Informationsfreiheit](https://www.datenschutz-hamburg.de/wir-ueber-uns-kontakt/wie-erreichen-sie-uns.html) (Hamburg Commissioner for Data Protection and Freedom of Information).

One last thing: This declaration applies to all digital products and services of the SPIEGEL Group. When we link to other websites, we have no influence and no control over whether the service provider complies with data protection provisions. If you wish to raise possible problems on a linked site or with one of our partners, please email us.

**10 | Details about your rights**

**GDPR Article 15: Data Subject Access Rights**You have the right to obtain information from us about the personal data we process.

**GDPR Article 16: Right of rectification**If the data concerning you is inaccurate or incomplete, you may request the rectification of incorrect information or the completion of incomplete information.

**GDPR Article 17: Right to erasure**In accordance with Art. 17 of GDPR, you can request the erasure of your personal data. Your right to erasure depends, among other things, on whether the data concerning you is still needed by us to fulfil our legal or contractual obligations.

**GDPR Article 18: Right to restriction of processing**In accordance with Art. 18 of GDPR, you have the right to request that the processing of personal data concerning you be restricted.

**GDPR Article 21: Right to object**For reasons relating to your particular situation, you have the right to object to the processing of personal data concerning you at any time.

**Art. 7 para. 1 of GDPR: Right to withdraw consent**You have the right to withdraw your consent for the processing of your personal data at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Version: 2020.002

Date: February 15, 2020

**11 | Details on individual services**

Our websites use the measurement procedure known as "next-generation innovative scalable central measurement process," or SZMnG, from [INFOnline GmbH](https://www.infonline.de/) for calculating key statistical figures on the usage of our products and services. The goal of usage measurement is to statistically determine the number of visits to our websites, the number of website visitors and their surfing behavior – on the basis of a uniform standard procedure – and so obtain values that are comparable across the market. For all digital products and services that are members of the Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. ([IVW](http://www.ivw.eu/); German Audit Bureau of Circulation) or take part in studies of the Arbeitsgemeinschaft Online-Forschung e.V. ([AGOF](http://www.agof.de/); Working Group for Online Media Research), usage statistics on reach are regularly processed further by AGOF and the Arbeitsgemeinschaft Media-Analyse e.V. ([agma](http://www.agma-mmc.de/); Media Analysis Working Group) and published with the performance value "unique user" as well as the performance values "page impression" and "visits" from IVW. These reach values and statistics can be seen on the respective websites.

**1. Legal basis for processing**

Measurement using INFOnline GmbH's SZMnG process is carried out on the basis of legitimate interest as defined by Art. 6, para 1, lit. f of the GDPR. The purpose of processing personal data is the generation of statistics and the formation of user categories. The statistics help us understand and verify the usage of products and services. The user categories form the basis for provision of advertising material and/or advertising measures aligned with your interests. For the marketing of our website, usage measurement that guarantees comparability with other market participants is essential. Our legitimate interest arises from the economic usability of the findings generated by statistics and user categories and the market value of our website – including direct comparison with the websites of third parties – which can be determined using statistics. Moreover, we have a legitimate interest in making available the pseudonymized data from INFOnline, AGOF, agma and IVW for the purposes of market research (AGOF, agma) and for statistical purposes (INFOnline, IVW). Moreover, we have a legitimate interest in making available the pseudonymized data from INFOnline for further development and provision of advertising materials aligned with interests.

**2. Type of data**

INFOnline GmbH collects the following data which, according to the GDPR, may contain references to individuals:

* IP address: Every device on the Internet requires a unique address for the transfer of data – the IP address. Because of the way the Internet works it is a technical requirement that the IP address be stored at least in the short term. IP addresses are reduced by 1 byte before any processing and only processed further anonymously. There is no saving or further processing of non-truncated IP addresses.
* A randomly generated client identifier: To identify computer systems, reach processing uses either a third-party cookie, a first-party cookie, a "local storage object" or a signature generated from a range of information automatically transferred by your browser. This identifier can uniquely identify a browser as long as the cookie or local storage object is not deleted. Measurement of data and subsequent allocation to the relevant client identifier is therefore also possible if you access other websites that use INFOnline GmbH's measurement process ("SZMnG").

The validity of cookies is restricted to a maximum of one year.

**3. Usage of data**

INFOnline GmbH's measurement process, which is used on this website, communicates usage data. This occurs for the collection of the performance values "page impressions," "visits" and "clients" and to generate other key figures from them (e.g. qualified clients). Moreover, we may use the measurement data as follows:

* "Geo-localization," the allocation of website access to the location from which it was accessed, occurs solely on the basis of the anonymized IP address and only to the geographical level of state/region. The geographic information gathered in this way can never be used to allow deduction of a user's precise whereabouts.
* The usage data of a technical client (e.g. a browser on a device) is compiled across websites and stored in a database. This information is used for technical estimation of the demographic details of age and sex and transferred to the AGOF service provider for further reach processing. As part of the AGOF study, a random sample of social characteristics is used to provide a technical estimate that allows assignment to the following categories: age, sex, nationality, profession, marital status, general household details, household income, place of residence, Internet usage, online interests, usage location, user type.

**4. Storage duration of the data**

INFOnline GmbH does not store the complete IP address. The truncated IP address is stored for a maximum of 60 days. The usage data in connection with the unique identifier is stored for a maximum of six months.

**5. Transfer of data**

Neither the IP address nor the truncated IP address is transferred. In generating the AGOF study, data is transferred to the following AGOF service providers with client identifiers:

* [Kantar Deutschland GmbH](https://www.tns-infratest.com/)
* [Ankordata GmbH & Co. KG](http://www.ankordata.de/homepage/)
* [Interrogare GmbH](https://www.interrogare.de/)

**6. Rights of data subjects**

Data subjects have the following rights:

* Right of access (Art. 15 GDPR)
* Right to rectification (Art. 16 GDPR)
* Right to object (Art. 21 GDPR)
* Right to erasure (Art. 17 GDPR)
* Right to restriction of processing (Art. 18 et seq. GDPR)
* Right to data portability (Art. 20 GDPR)

For any inquiries related to these rights, please contact [datenschutz@spiegelgruppe.de](mailto:datenschutz@spiegelgruppe.de). Please note that for this type of inquiry, we must be able to establish that we are dealing with the data subject. The data subject has the right to lodge a complaint with the data protection authorities. You can find further information on the measurement process on the website of [INFOnline GmbH](https://www.infonline.de/), which operates the measurement process, the data protection website of [AGOF](http://www.agof.de/) and the data protection website of [IVW](http://www.ivw.eu/).

**About Our Partnership with IP Deutschland GmbH**

**1) Overview**

Various companies are involved in the marketing of our Internet products and services, both in the collection of data and in the serving of advertising. These companies play different roles. In some cases, they are individually responsible for data processing (controller) or act purely as a service provider carrying out the instructions of a controller (processor). In the context of advertising marketing, IP Deutschland GmbH, Picassoplatz 1, 50679 Cologne, Germany, e-mail: [kontakt@ip.de](mailto:kontakt@ip.de) , is responsible and are thus, together with us, "joint controllers" under Article 26 of the EU General Data Protection Regulation in terms of our internet products and services. You can find more details about this, about roles and about other responsible parties [here](http://www.ip.de/informationen_externe_vermarktung).

**2) Collection of data in the context of marketing (tracking, profiling, etc. …)**

In order to personalize advertising, design it according to interests and find suitable target groups, to collect information for billing, measure reach and control/limit the serving of ads through frequency capping, a system is used in online advertising that examines user behavior and produces pseudonymized profiles of users, which can then be used in the serving of advertising. As part of that process, products and services that have been visited, content that has been clicked on, etc., are captured and stored. This data is stored within a profile in a database that can be accessed with a cookie or by another means of identification. Names and personal data of users are not stored. The cookie is essentially a pseudonym and does not contain the real name or identity of the user. In some cases, data from other sources, e.g. parts of profiles from registered areas or also technical data about the device used, the time the activity occurred or data from party sources can also be stored. Behavior patterns of users of our products and services are stored and analyzed within the profile and it is in part supplemented by sociodemographic data or assumptions about sociodemographic data (so-called statistical twins of profiles with known data that are compared based on similar or identical surfing behavior). The formation of this profile is also possible across networks, i.e. across a number of internet products or services.

**3) Legal basis**

Both the operators of the products and services and the other marketers and other entities that serve advertising on the products and services have a legitimate interest in marketing and monetizing their (marketed) products and services through the target group-specific serving of advertising as well as measuring the reach and controlling the serving of advertising with the use of frequency capping. The same applies to the creation of user profiles that make this possible in the first place. This purpose could not be achieved without data processing. Given the pseudonymous nature of the data, users of the products and services will not be individually identifiable to us or our marketers beyond the recognition of the browser and end devices used. Incursions on the user's right of informational self-determination are justified by the fact that the user's data is pseudonymized and is only used for relatively short periods of time. Because users are informed transparently of the procedures used in data protection statements and are also provided with effective possibilities for opting out, incursions on users' rights are minimal and at the expected level. Furthermore, no profiles are produced that focus on children. The legal basis for all processing of data in the scope of marketing is Art. 6 1f of the GDPR ("legitimate interests") or § 15, para. 3 of the German Telemedia Act (Telemediengesetzt).

**4) Detailed information about options for objecting**

* Information about marketers and technology opt-out opportunities

[Here](http://www.ip.de/informationen_externe_vermarktung), you can find detailed information about the individual data processing procedures and the service providers and participants involved. This overview contains general and detailed information about the names and addresses of the companies that collect, process and/or make personal data available to other third parties, the data categories collected, the purpose of processing and the opt-out options, recipients of data, transfer to third countries, duration of storage and data sources and provides the ability to contact the data protection officer of IP Deutschland GmbH.

* Advertising IDs for mobile apps

To enable advertisements to be delivered in services that lack cookie technology – in mobile apps, for example – technologies similar to cookies may be employed. To disable personalized advertising on your mobile device, please follow the instructions below.

**Android**

1. Depending on the device, you will find Google Settings at one of the following places:

a. in a separate app called Google Settings

b. scroll through your main Settings app and tap Google

2. Tap on Ads

3. Tap the on-off slider to deactivate personalized ads

**iOS**

iOS devices use Apple's Advertising Identifier. You can find further information about the different possibilities for using this identifier in the app settings on your device.

You can find it as follows:

1. Tap "Settings"

2. Tap "Privacy"

3. Tap "Advertising." From there, you select specific settings using a slider.

**Right to object**

Should you not wish to take part in measurement on websites, you can object at the following link: [https://optout.ioam.de](https://optout.ioam.de/). For technical reasons a cookie must be set to guarantee your exclusion from measuring. Should you delete the cookies in your browser, you will need to repeat the opt-out process at the link above. In applications, you can opt out of this measuring here; in apps you can deactivate them in settings (for iOS in iOS Settings > App > AGOF-Zählung, for Android directly in the app menu under Data protection > IVW/AGOF-Zählung).

**Opinary GmbH**

We embed a survey tool from Opinary GmbH, Engeldamm 62-64, 10179 Berlin, Germany, on our pages.

The use of this service allows us to create and display online polls or other content. The Opinary plugin retrieves the following information from the website visitor: Cookie IDs, timestamps, click data, vote coordinates and truncated IP addresses. For the protection of your personal data, we have an agreement with Opinary GmbH on the order in which this data is processed (Art. 26, GDPR). As part of our joint responsibility under data protection law, it was agreed which party would fulfil which obligations under the GDPR.

We are the responsible party for the collection and transmission of the user’s data to Opinary. The data collected in this way is then anonymized by Opinary and made available to us in aggregated form.

In order to control target group based advertising, Opinary collects information about activities on our websites (advertising banners clicked and subpages visited, for example) under a pseudonym and uses this information to serve you advertising from third parties in line with your interests. This allows cookies from third-party advertisers to be stored on your computer.