VORLAGE

Richtlinie zu Datenschutzverletzungen in Deutschland (DE)

Versionsverlauf

Version	Änderungs-datum	Änderungs-notiz	Bearbeiter (Name/Rolle)	Überprüfuer (Name/Rolle)	Veröffentlichungs-datum	Datum der nächsten Überprüfung

Diese Richtlinie wird [monatlich, vierteljährlich, jährlich] überprüft.

1. Einführung

1.1 Zweck dieser Richtlinie

In dieser Richtlinie werden die Rollen und Verantwortlichkeiten für die Benachrichtigung, Bearbeitung und Eskalation von Verstößen gegen den Schutz personenbezogener Daten klar dargelegt, um die geschäftlichen Auswirkungen wie finanzielle Verluste oder andere Konsequenzen (siehe unten) zu minimieren, eine angemessene Kommunikation sicherzustellen, konsistent zu reagieren, die Reaktionszeiten zu verkürzen und die entsprechenden Maßnahmen zu ergreifen, Verstöße gegen den Schutz personenbezogener Daten ordnungsgemäß zu beseitigen.

Folgen von Datenschutzverletzungen:

- Die EU-Datenschutz-Grundverordnung (EU-DSGVO) sieht im Falle eines Datenschutzverstoßes Bußgelder von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes eines Unternehmens vor.
- Es drohen Reputationsschäden und Reputationsverluste.
- Die wissentliche, gewerbsmäßige und unbefugte Offenlegung zahlreicher personenbezogener Daten kann mit einer Freiheitsstrafe bis zu drei Jahren oder einer Geldstrafe geahndet werden. Für die missbräuchliche Verwendung von Daten oder die unerlaubte und entgeltliche Datenverarbeitung bleibt der bisherige Strafrahmen bestehen.
- Es drohen Schadensersatzansprüche der Betroffenen in unbegrenzter Höhe.

Diese Richtlinie legt das Verfahren und die Schritte fest, die bei der Behandlung und Reaktion auf eine (potenzielle) Verletzung des Schutzes personenbezogener Daten befolgt werden müssen.

1.2 Zielgruppe dieser Richtlinie

Diese Richtlinie gilt für alle [Mitarbeiter, Auftragnehmer...] im Falle einer (potenziellen) Verletzung des Schutzes personenbezogener Daten.

„Wir“, wie in dieser Richtlinie verwendet, bezeichnet alle Mitarbeiter, Auftragnehmer und[Name des Unternehmens] selbst.

1.3 Umfang dieser Richtlinie

Diese Richtlinie deckt Verstöße gegen den Schutz personenbezogener Daten im Zusammenhang mit den einschlägigen Datenschutzgesetzen ab.

2. Terminology Explanation & Examples of Data Breaches

Eine Verletzung des Schutzes personenbezogener Daten kann allgemein als ein Sicherheitsvorfall definiert werden, der die Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten beeinträchtigt hat. Verletzungen des Schutzes personenbezogener Daten können durch unbefugte oder unbeabsichtigte Offenlegung, unsachgemäße Datenentsorgung, Kontrollverlust oder Diebstahl von Daten, menschliches Versagen im Zusammenhang mit Daten oder Angriffe Dritter verursacht werden.

Bei personenbezogenen Daten muss es sich um Informationen handeln, die sich auf eine Person beziehen, und die Person muss entweder direkt oder indirekt anhand eines oder mehrerer für die Person spezifischer Faktoren identifiziert oder identifizierbar sein.

Beispiele für Datenschutzverletzungen finden Sie in dieser Richtlinie in Anhang 2.

3. Verantwortung

Wir, [Name des Unternehmens], sind als Datenverantwortlicher dafür verantwortlich, Verstöße gegen den Schutz personenbezogener Daten der zuständigen Behörde zu melden. Um eine angemessene Kommunikation zu gewährleisten, konsistent zu reagieren und die Reaktionszeiten zu verkürzen und um Verletzungen des Schutzes personenbezogener Daten ordnungsgemäß zu behandeln, haben wir festgelegt, wer für die relevanten Prozesse innerhalb von [Name des Unternehmens] verantwortlich ist, wie unten angegeben:

Verantortlichkeitsbereich	Verantwortliche Person (Name/Rolle)	Stellvertreter der Hauptperson (Name/Rolle)	Zugewiesen am (Datum)	Aktualisiert am (Datum)
Bewertung, ob personenbezogene Daten in den Vorfall involviert sind				
Beurteilung, ob der Vorfall wahrscheinlich ein hohes Risiko darstellt				
Mitarbeiterschulung und Sensibilisierung für Datenschutzverletzungen				
Benachrichtigung der zuständigen Behörde				
Benachrichtigung betroffener Datensubjekte				
Benachrichtigung anderer beteiligter Parteien				

4. Umgang mit (potenziellen) Datenschutzverletzungen

Wir stellen sicher, dass wir alle Verstöße protokollieren, unabhängig davon, ob sie der zuständigen Behörde oder den betroffenen Personen gemeldet werden müssen oder nicht

4.1 Qualifizierung, ob der Vorfall personenbezogene Daten lebender Personen betrifft.

Bei personenbezogenen Daten muss es sich um Informationen handeln, die sich auf eine Person beziehen, und die Person muss entweder direkt oder indirekt anhand eines oder mehrerer für die Person spezifischer Faktoren identifiziert oder identifizierbar sein.

4.2 Bewerten Sie, ob die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten des Einzelnen darstellt.

Wir verwenden das Formular zur Meldung von Datenschutzverletzungen (siehe*Anhang 1)*, um Informationen über den Vorfall zu sammeln, und beziehen unser Team [DSB, Recht, Compliance usw.] ein, um bei der Bewertung des Risikos des Vorfalls und bei der Entscheidung, ob eine Benachrichtigung erforderlich ist, zu helfen.

5. Benachrichtigung

5.1 Benachrichtigen Sie die betroffenen Personen

Wenn festgestellt und dokumentiert wird, dass der Verstoß voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, müssen Wir in der Rolle des Datenverantwortlichen die betroffene(n) Person(en)**direkt und unverzüglich benachrichtigen**. Wir sollten sie in klarer und verständlicher Sprache darüber informieren:

- Die Art der Verletzung des Schutzes personenbezogener Daten,
- Die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- Alle ergriffenen oder vorgeschlagenen Schritte zur Bewältigung des Verstoßes gegen den Schutz personenbezogener Daten und zur Abmilderung der Auswirkungen des Verstoßes,
- Unser Name und die Kontaktdaten der Kontaktstellen, bei denen weitere Informationen erhältlich sind,
- Die Kontaktdaten unseres Datenschutzbeauftragten (DPO),
- Der Name der zuständigen Behörde und
- Geben den betroffenen Personen Ratschläge, was sie tun können, um sich zu schützen.

Wenn möglich, sollten Wir Einzelpersonen konkret und klar beraten, welche Maßnahmen sie ergreifen können, um sich zu schützen, und was Wir zu tun bereit sind, um ihnen zu helfen. Abhängig von den Umständen kann dies Folgendes umfassen:

- Erzwingen eines Zurücksetzens des Passworts;
- Einzelpersonen raten, sichere, eindeutige Passwörter zu verwenden; und
- Sie werden aufgefordert, auf ihren Konten nach Phishing-E-Mails oder betrügerischen Aktivitäten Ausschau zu halten.

Wenn es mit einem unverhältnismäßigen Aufwand verbunden ist, die betroffene(n) Person(en) direkt zu benachrichtigen (z. B. wenn die Kontaktdaten der betroffenen Personen nicht vorhanden sind), werden Wir alternative Möglichkeiten in Betracht ziehen, um die Betroffenen darauf aufmerksam zu machen (z. B. eine Erklärung auf der Website). .

Wenn Wir uns dazu entschließen, Einzelpersonen nicht zu benachrichtigen, müssenWir trotzdem die zuständige Behörde benachrichtigen, es sei denn, Wir können nachweisen, dass der Verstoß wahrscheinlich nicht zu einem Risiko für Rechte und Freiheiten führt. Die zuständige Behörde hat die Befugnis, uns zu verpflichten, betroffene Personen zu informieren, wenn Wir der Ansicht sind, dass ein hohes Risiko besteht.

5.2 Benachrichtigung der zuständigen Behörde

Wenn festgestellt und dokumentiert wird, dass der Verstoß voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, müssen Wir als Datenverantwortlicher die zuständige Behörde **innerhalb von 72 Stunden nach Kenntnisnahme** des Vorfalls und des (potenziellen) Datenlecks personenbezogener Daten benachrichtigen.

In [Deutschland] ist die zuständige Behörde […].

Auf der Grundlage der Informationen im vom Datenverantwortlichen bereitgestellten Formular für Datenschutzverletzungen wird die zuständige Behörde die verantwortliche Person kontaktieren, um Informationen über die nächsten Schritte zu geben. Es ist wahrscheinlich, dass die Behörde ein Aktenzeichen vergibt.

5.3 Zusätzliche Benachrichtigungen

Es ist wichtig, sich darüber im Klaren zu sein, dass Wir möglicherweise aufgrund anderer Gesetze zusätzlichen Meldepflichten unterliegen, wenn es bei uns zu einer Verletzung des Schutzes personenbezogener Daten kommt. Zum Beispiel:

- Wenn Wir ein Kommunikationsdienstleister sind, müssen Wir die zuständige Behörde gemäß den Datenschutz- und elektronischen Kommunikationsvorschriften (PECR) innerhalb von 24 Stunden über jede Verletzung des Schutzes personenbezogener Daten informieren. Wir sollten ein PECR-Benachrichtigungsformular für Verstöße anstelle des DSGVO-Prozesses verwenden.
- Wenn Wir ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste sind, unterliegen wir gemäß der NIS-Richtlinie der Pflicht zur Meldung von Vorfällen. Diese sind unabhängig von der Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß den einschlägigen Datenschutzgesetzen. Wenn es bei uns zu einem Vorfall kommt, bei dem es sich auch um einen Verstoß gegen den Schutz personenbezogener Daten handelt, müssen Wir diesen trotzdem gesondert der zuständigen Behörde melden und sollten dafür das Datenschutzverfahren nutzen.

Möglicherweise müssen Wir auch darüber nachdenken, Dritte zu benachrichtigen, beispielsweise:

- Die Polizei (z. B. wenn es sich bei dem Verstoß um den Diebstahl von Geräten oder Daten handelte),
- Versicherer,
- Professionelle Körper,
- Eltern,
- Dritte (z. B. wenn sie von der Verletzung ebenfalls betroffen sind), Gemeinde, Bank- oder Kreditkartenunternehmen, die dazu beitragen können, das Risiko finanzieller Verluste für Einzelpersonen zu verringern.

6. Further Action

6.1 Kontrollen und Maßnahmen

Nach der Dokumentation (und Benachrichtigung) der (potenziellen) Datenschutzverletzung sollte das Formular zur Meldung von Datenschutzverletzungen überarbeitet werden, um strengere Kontrollen und Maßnahmen einzuführen. Diese sollten ebenfalls dokumentiert und umgesetzt werden, wie zum Beispiel:

- Korrekturlesen externer Kommunikation,
- Entfernen der „Autofill“-Funktionen für E-Mail-Empfänger,
- Anfordern der Löschbestätigung einer irrtümlich versandten E-Mail nach Kenntniserlangung.

6.2 Verwalten von Anfragen und Beschwerden betroffener Personen

Infolge eines Verstoßes kann es bei einem Unternehmen zu einem höheren Volumen an Datenschutzanfragen oder -beschwerden kommen, insbesondere im Zusammenhang mit Zugriffs- und Löschungsanfragen. Für diesen Fall sollte ein Notfallplan vorhanden sein.

Es ist wichtig, dass Wir diese Anfragen und Beschwerden weiterhin bearbeiten, zusammen mit allen anderen Arbeiten, die infolge des Verstoßes entstanden sind.

Wir sollten auch darüber nachdenken, wie Wir mit den Auswirkungen auf Einzelpersonen umgehen können, einschließlich der Erläuterung, wie sie eine Entschädigung beantragen können, wenn die Situation dies erfordert.

6.3 Verwandte Richtlinien

Falls noch nicht vorhanden, sollten weitere entsprechende Richtlinien erstellt, veröffentlicht und umgesetzt werden, zum Beispiel:

- Sicherheitsrichtlinie, die die Richtlinien und Prozesse zum Schutz personenbezogener Daten vor Verlust und Missbrauch festlegt.
- Die Datenschutzrichtlinie legt die Verpflichtungen gemäß den jeweils geltenden Datenschutzgesetzen (z. B. DSGVO) zur Verarbeitung personenbezogener Daten fest.

6.4 Protokoll/Register für Datenschutzverletzungen

Es gibt [noch kein] Protokoll/Register für Datenschutzverletzungen, das für jeden Fall aktualisiert wird.

6.5 Schulung und Bewusstsein

Vorbeugung ist immer besser als die Bewältigung und Eindämmung einer Verletzung des Schutzes personenbezogener Daten und ihrer Risiken. Bedenken in dieser Angelegenheit können jederzeit auftreten und jeder sollte seine Bedenken melden. Dies kann dazu beitragen, auftretende Risiken zu erkennen und zu erfassen, personenbezogene Daten vor (potenziellen) Datenschutzverletzungen zu schützen und die Prozesse auf dem neuesten Stand und effektiv zu halten.

Relevante Schulungen für Mitarbeiter und Auftragnehmer zur Aufklärung und Sensibilisierung werden[nicht] auf [monatlicher, vierteljährlicher, jährlicher] Basis angeboten.

7. Anhang 1: Formular zur Meldung von Datenschutzverletzungen

Bitte fragen Sie Ihren DataGuard-Experten oder besuchen Sie den Abschnitt „Ressourcen“ auf Ihrer DataGuard-Plattform, um das Formular zur Meldung von Datenschutzverletzungen zu finden.

8. Anhang 2: Beispiele für Verstöße gegen den Schutz personenbezogener Daten

8.1 Beispiel 1: Versehentliches Versenden einer Datei per E-Mail

- Eine E-Mail mit sensiblem Inhalt wird an eine unbegrenzte Anzahl von Personen gesendet.

8.2 Beispiel 2: Medikamente an den falschen Patienten schicken

[Beispiel]

8.3 Beispiel 3: Unterlassene Schwärzung personenbezogener Daten und Benachrichtigung

[Beispiel]

8.4 Beispiel 4: Phishing-Angriff

[Beispiel]

8.5 Beispiel 5: Verlorene oder gestohlene Daten

- Bei einem Hackerangriff werden personenbezogene Daten gestohlen.
- Laptop wird in einem Auto gestohlen.
- Verlust von Hardware, die personenbezogene Daten enthält (USB-Sticks, geschäftlich genutztes oder privat genutztes Mobiltelefon, Notebook etc.).

8.6 Beispiel 6: Offenlegung von Daten

- Kreditkartendaten sind im Internet offen verfügbar.

8.7 Beispiel 7: Falsche Entsorgung

- Patientenakten werden im Hausmüll entsorgt.