INTERNATIONALE HOCHSCHULE

Datenschutz & IT-Sicherheit
SoSe 2023

DSBDSITS01

DATENSCHUTZ UND IT-SICHERHEIT

Virtuell in Bielefeld,
Leipzig, Hannover
uvm.

AGENDA

Begriffsbestimmungen und Hintergründe	**01**	04./05.04.
Grundlagen des Datenschutzes	**02**	12./19./26.04.
Grundlagen der IT-Sicherheit	**03**	02./03.05.
Standards und Normen der IT-Sicherheit	**04**	17./31.05.
Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz	**05**	07./14.06
Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte	**06**	20./21.06.
Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen	**07**	28.06./05.07.
Recap, Q&A, Besprechung der Übungsklausur	**08**	12.07.

“Am Ende liegt es an uns selbst: Es ist nicht die Aufgabe oder die Verantwortung von jemand anders, sondern die der Bürger unseres Landes und der Bürger der Welt, den Kurs der Geschichte hin zur Gerechtigkeit zu lenken. […] Deshalb ist das wichtigste Amt in jedem Land nicht das des Präsidenten oder Regierungschefs, der wichtigste Titel ist der des Bürgers. […] In allen unseren Ländern werden es immer unsere Bürger sein, die darüber entscheiden, was für Länder wir sind, welche Ideale wir anstreben und welche Werte uns prägen”

- Barack Obama

(am 16.11.2016 in einer Grundsatzrede in Griechenland)

RELEVANZ DES DATENSCHUTZES AM BEISPIEL

Verstöße gegen EU-Datenschutz

Rekordstrafe gegen Meta: 1,2 Milliarden Euro

22.05.2023 11:23 Uhr

Die Facebook-Mutter Meta hat sich offenbar nicht an ein Urteil gehalten daten an die USA übermittelt haben. Dafür kassiert Meta nun eine Reko

Nach Datenschutz-Bedenken

ChatGPT wieder in Italien erlaubt

28.04.2023 22:46 Uhr

Menschen in Italien können ChatGPT wieder nutzen. Die italienische Datenschutzbehörde hatte die KI-Software zuvor verboten.

Quelle: https://www.zdf.de/nachrichten/wirtschaft/meta-milliarden-strafe-eu-datenschutz-verstoesse-100.html / https://www.zdf.de/nachrichten/digitales/chat-gpt-italien-100.html

AGENDA

Begriffsbestimmungen und Hintergründe	**01**	18.04
Grundlagen des Datenschutzes	**02**	25.04./ 30.05. /06.06.
Grundlagen der IT-Sicherheit	**03**	27.06.
Standards und Normen der IT-Sicherheit	**04**	04.07.
Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz	**05**	11.07.
Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte	**06**	18.07.
Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen	**07**	25.07.

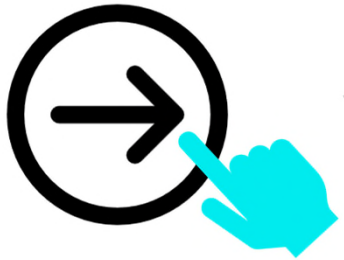
LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, …

- … welche Konzepte und Prinzipien im Datenschutz Anwendung finden
- … welche rechtlichen Vorgaben zum Datenschutz in Deutschland zu beachten sind
- … was die wichtigsten gesetzlichen Grundlagen des Datenschutzes sind
- … wie Datenschutz in der praktischen Umsetzung anzuwenden ist

EINFÜHRUNG

Übung: Beispiel



5 Minuten - Abstimmung

(Password: DaSchu_ITS_24)

- Eine Frau wehrt sich gegen die **Absage einer Sicherheitsfirma** wegen fehlender charakterlicher Eignung, die mit Verweis auf anonym zugespielte Bilder und Texte aus einem Internetforum begründet wurde.
- In dem Internetforum beschrieb die Frau, dass sie sich regelmäßig an Glücksspielen beteiligt, teilweise auch um große Summen. Die Frau erwähnte in diesem Internetforum unzutreffender Weise auch, dass sie bereits Mitarbeiterin der Sicherheitsfirma sei.
- Wurde der Frau zu Unrecht abgesagt?

- Ein Unternehmen speichert den gesamten E-Mail-Verkehr mit seinen Kunden im Rahmen der Bearbeitung der Bestellungen. Er wird später von einem Kunden wegen fehlerhafter Lieferung verklagt. Das Unternehmen legt den E-Mail-Verkehr mit diesem Kunden im Prozess zu seiner Verteidigung vor.

02

GRUNDLAGEN DES DATENSCHUTZES

THEMEN

- Fokus Konzepte & Prinzipien
- Fokus Recht
- Fokus Praxis

“Datenschutz ist Machtkontrolle, Datenschutz ist Schutz des Individuums, Datenschutz ist Schutz der Freiheit, Datenschutz ist Schutz der informationellen Selbstbestimmung.“

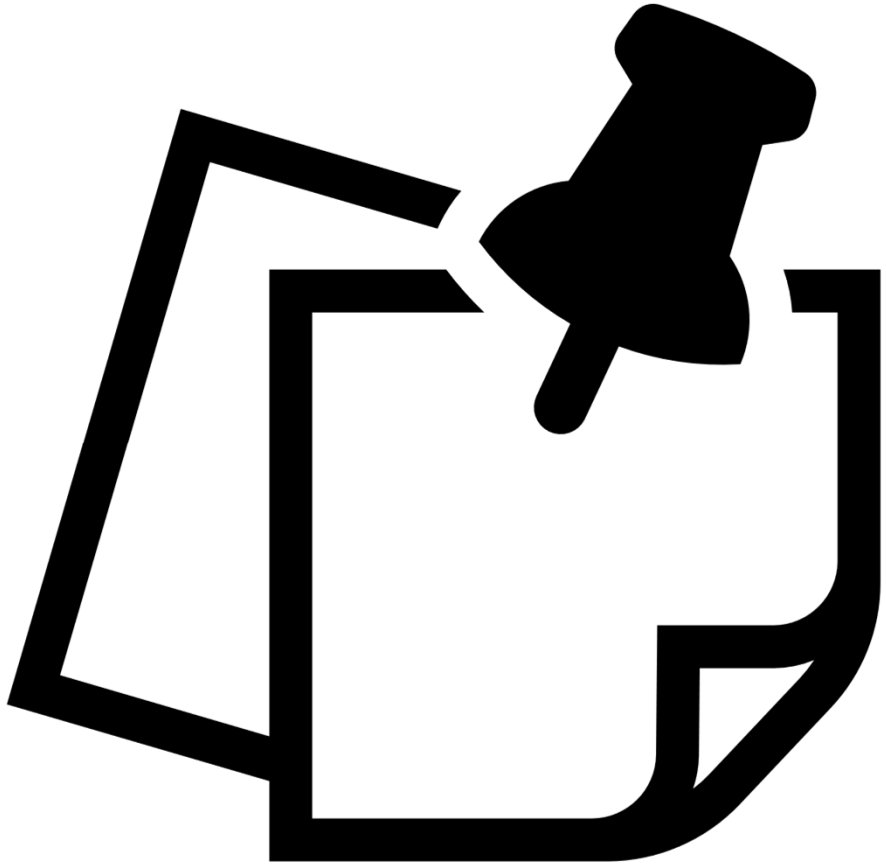
- Karl Michael Betzl

(Deutscher Jurist, Landesdatenschutzbeauftragter des Freistaats Bayern 2006)

DEFINITION:
PERSONENBEZOGENE DATEN & BETROFFENE PERSON

*„**personenbezogene Daten**“ [bezeichnet] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person*

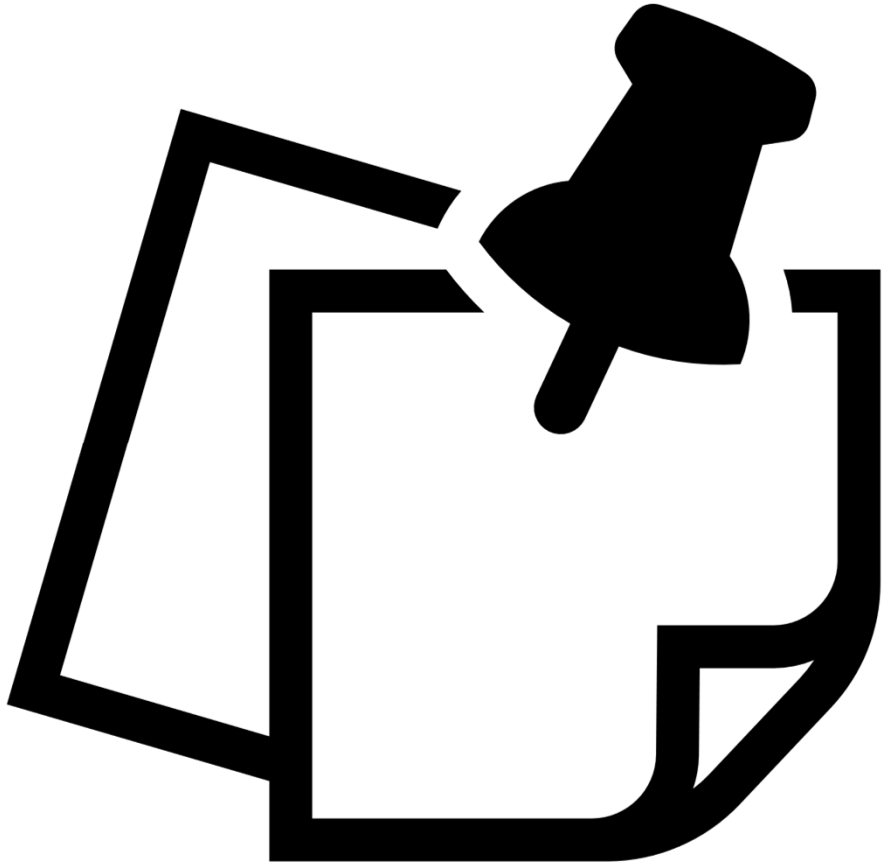
*(im Folgenden „**betroffene Person**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *VERARBEITUNG*

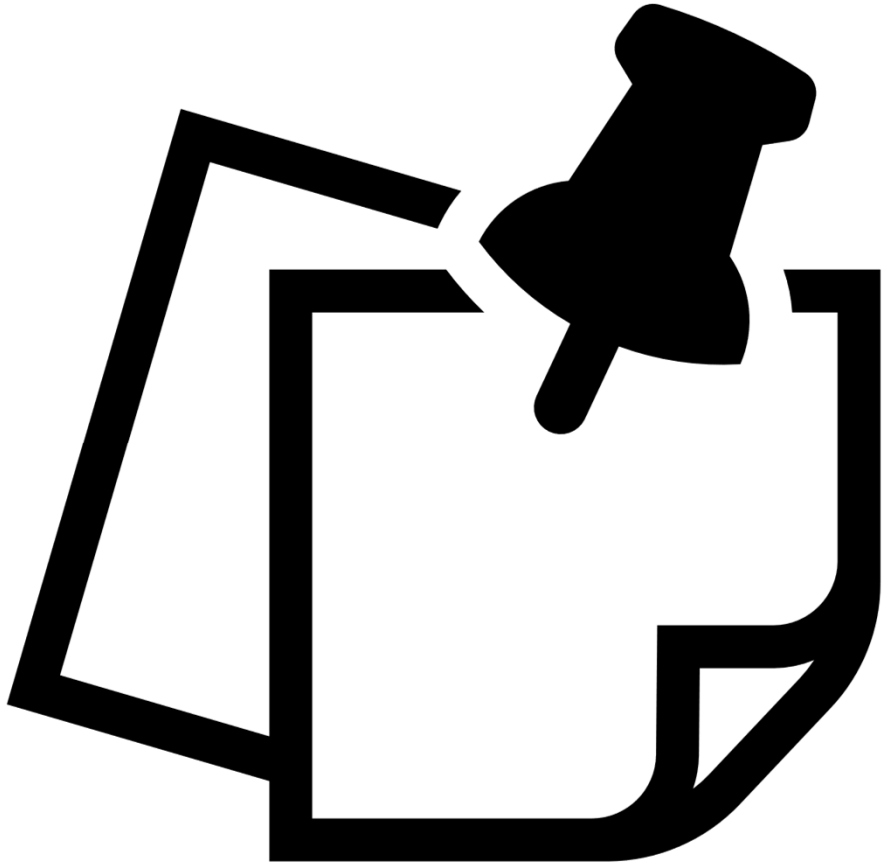
*„**Verarbeitung**“ [bezeichnet] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *VERANTWORTLICHER*

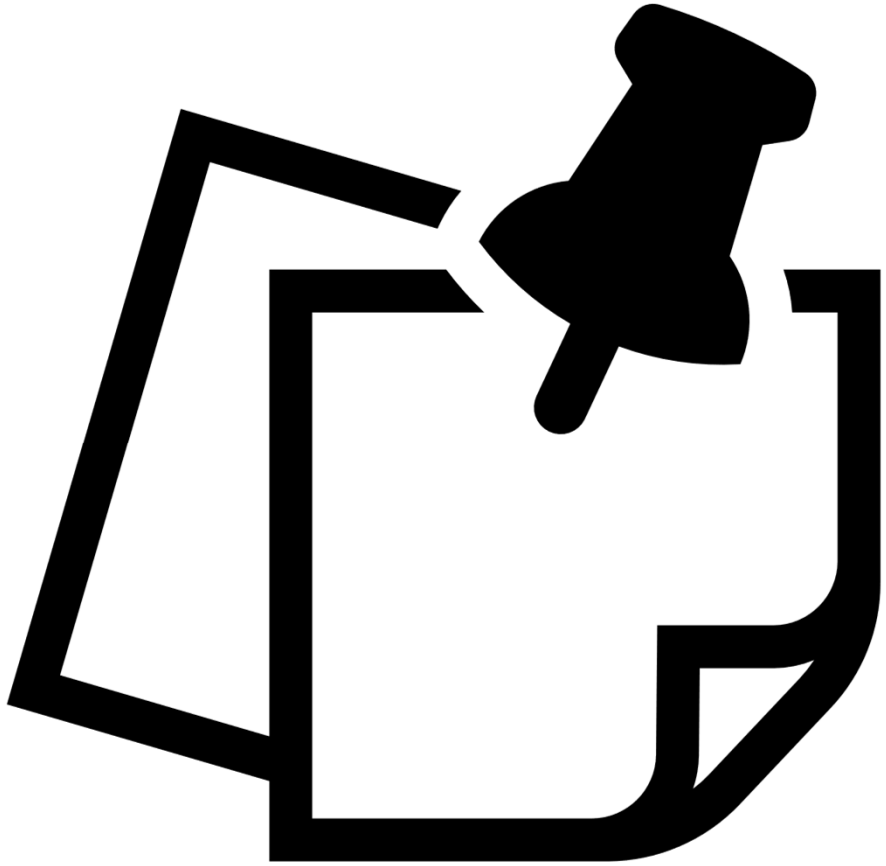
*„**Verantwortlicher**“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *AUFTRAGSVERARBEITER*

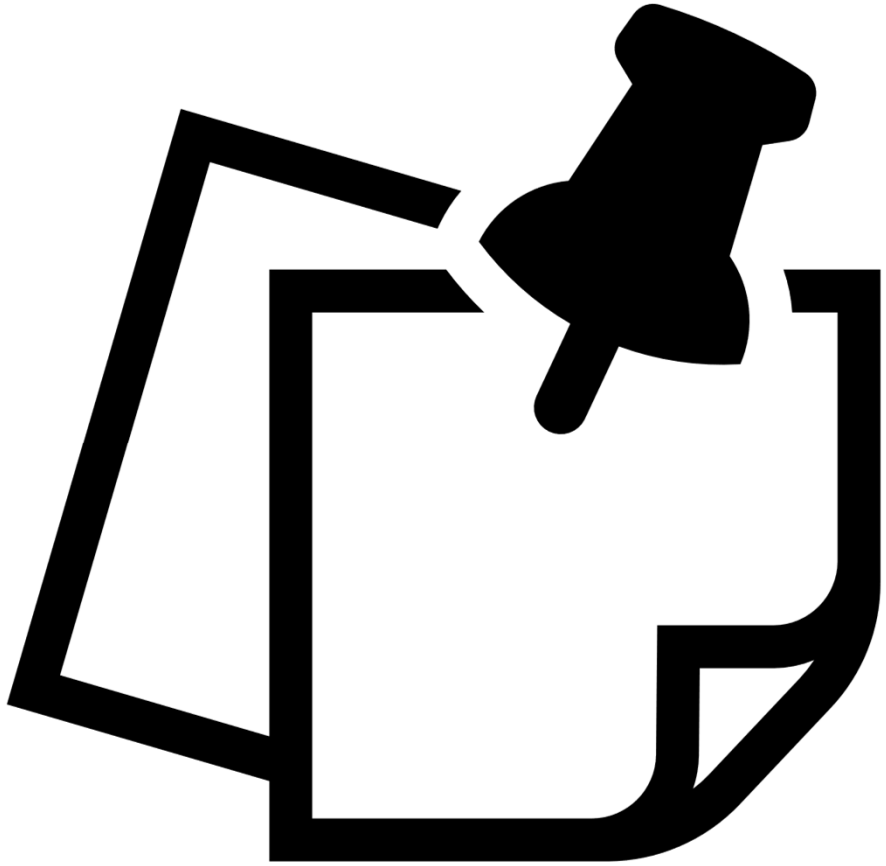
*„**Auftragsverarbeiter**“ [bezeichnet] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *DRITTER*

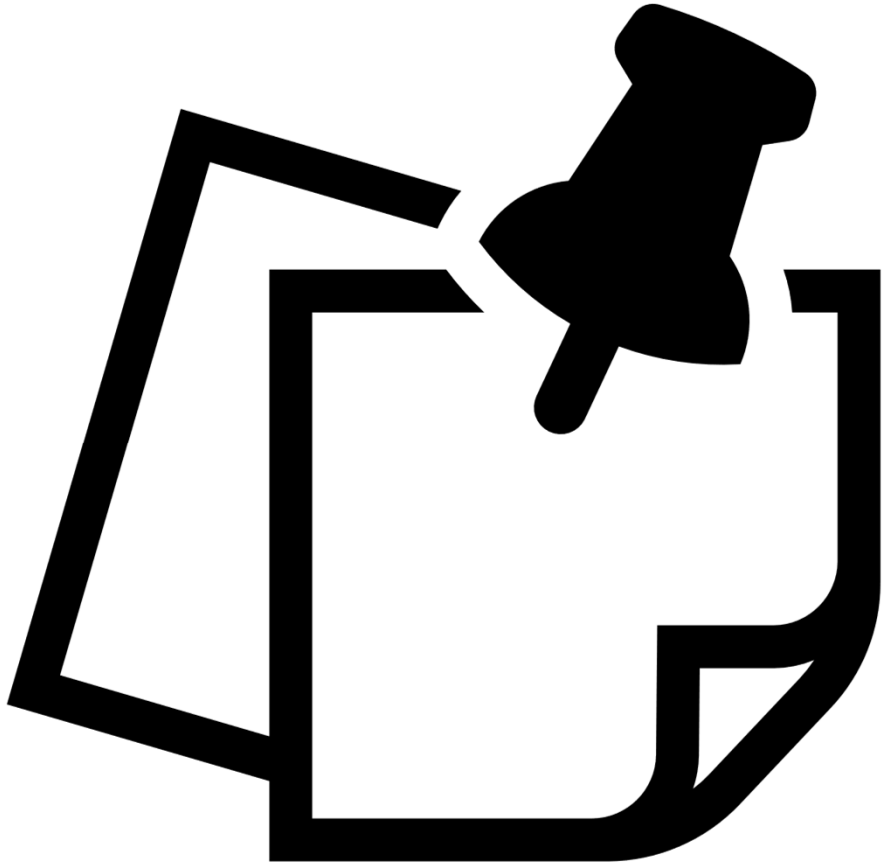
*„**Dritter**“ [bezeichnet] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *EMPFÄNGER*

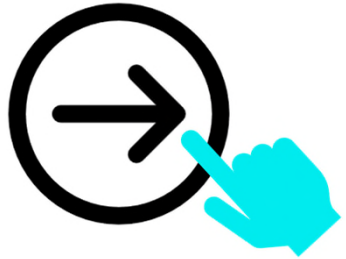
*„**Empfänger**“ [bezeichnet] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.*



Quelle: EU-DSGVO Artikel 4

DATENSCHUTZ

Übung: Personenbezogene Daten (PBD)



(Password: DaSchu_ITS_24)

30 Minuten - Gruppenarbeit

1) Nennen Sie fünf Beispiele von personenbezogenen Daten (die wenn möglich nicht auf der nächsten Folie zu finden sind)

2) Visualisieren Sie das Zusammenspiel von Verantwortlichem, Auftragsverarbeiter, Betroffenem und Drittem (in Miro).

3) Nutzen Sie eins Ihrer Beispiele von personenbezogenen Daten und entwerfen ein Fall, in dem alle vorgenannten Akteure vorkommen.

4) Vorstellung im Plenum (zufällige Gruppe)

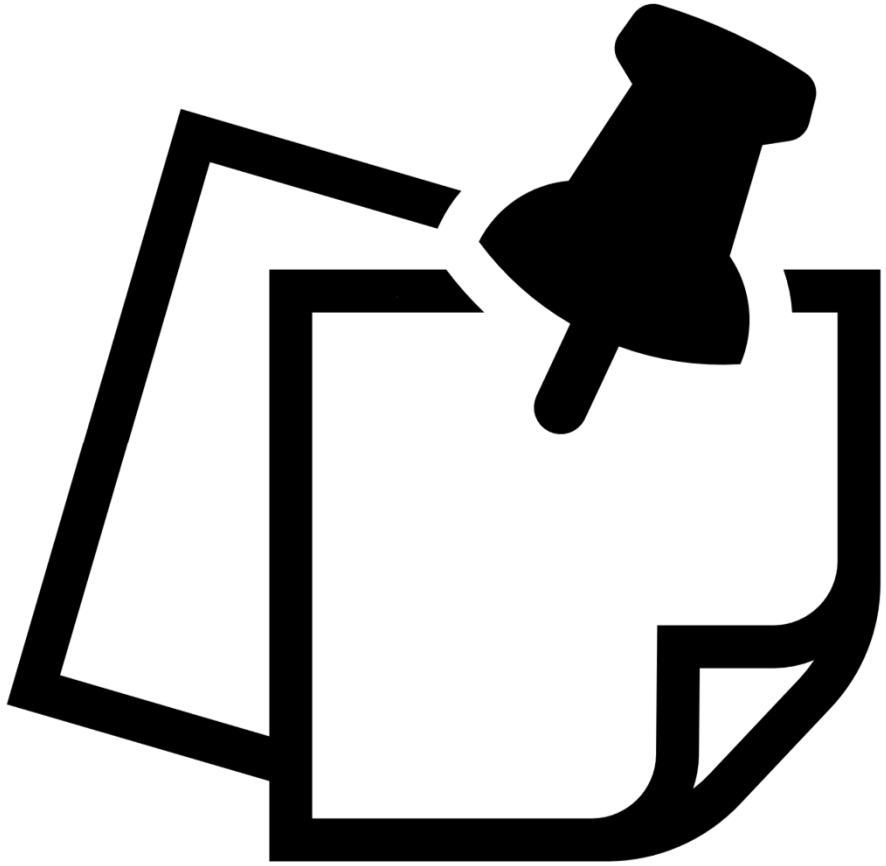
BEISPIELE FÜR PERSONENBEZOGENE DATEN

INTERNATIONALE HOCHSCHULE

Name	Adresse	E-Mail-Adresse	Telefonnummer
Geburtstag	Kontodaten	Kfz-Kennzeichen	Standortdaten
	IP-Adressen	Cookies	

DEFINITION: *PROFILING*

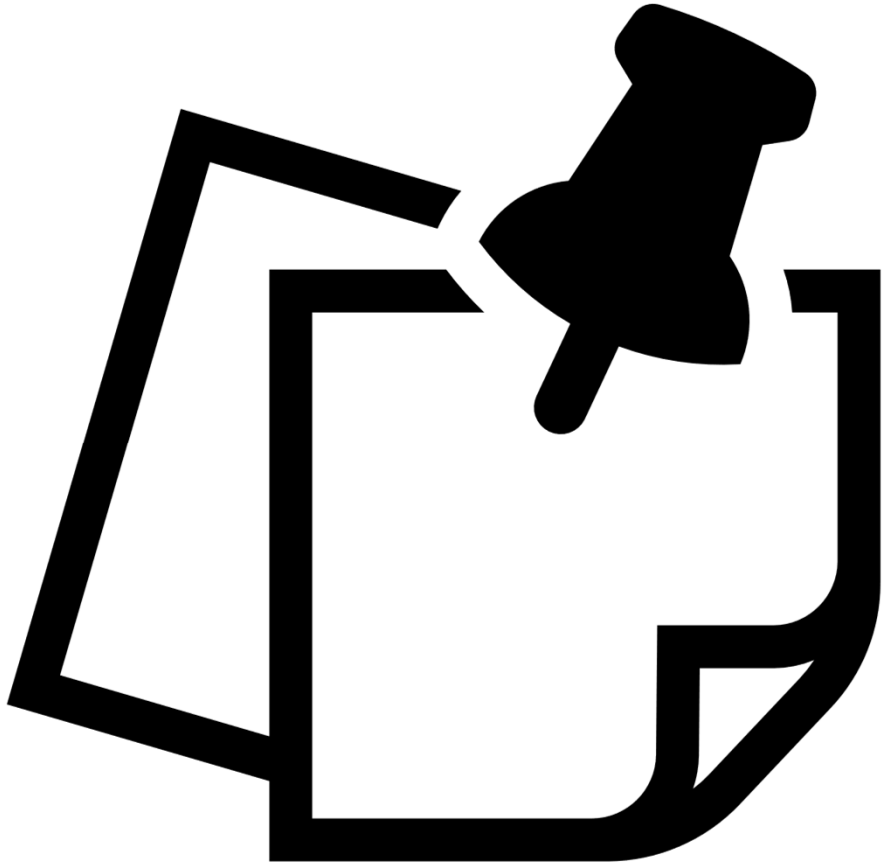
*„**Profiling**“ [bezeichnet] jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *PSEUDONYMISISERUNG*

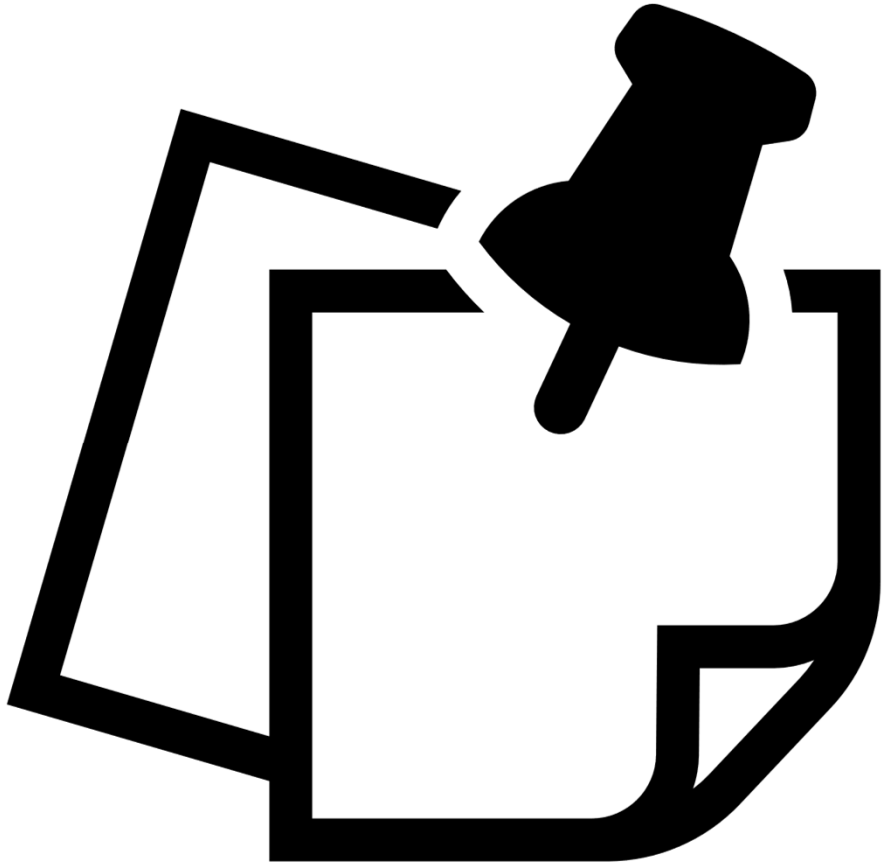
*„**Pseudonymisierung**“ [bezeichnet] die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.*



Quelle: EU-DSGVO Artikel 4

DEFINITION: *STAND DER TECHNIK*

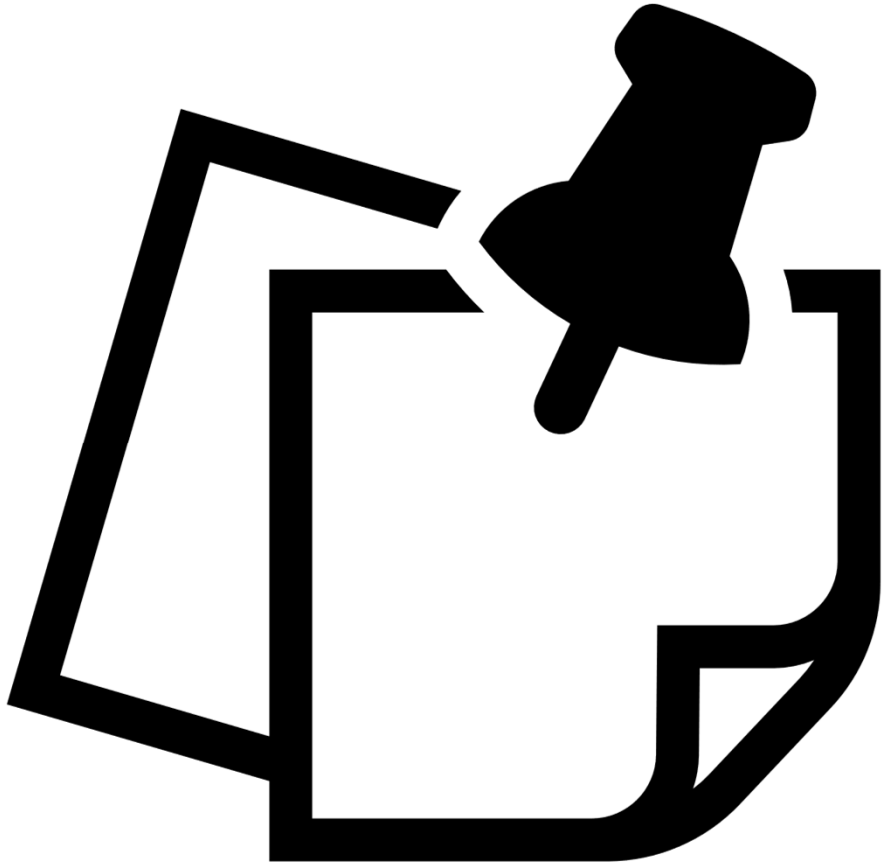
Entwicklungsstand technischer Systeme, der zur (vorsorgenden) Abwehr der (im zugrunde liegenden Gesetz beschriebenen) Gefahren geeignet und der verantwortlichen Stelle zumutbar ist.



Quelle: C. Witt (2010)

DEFINITION: *EFFEKTIVITÄT*

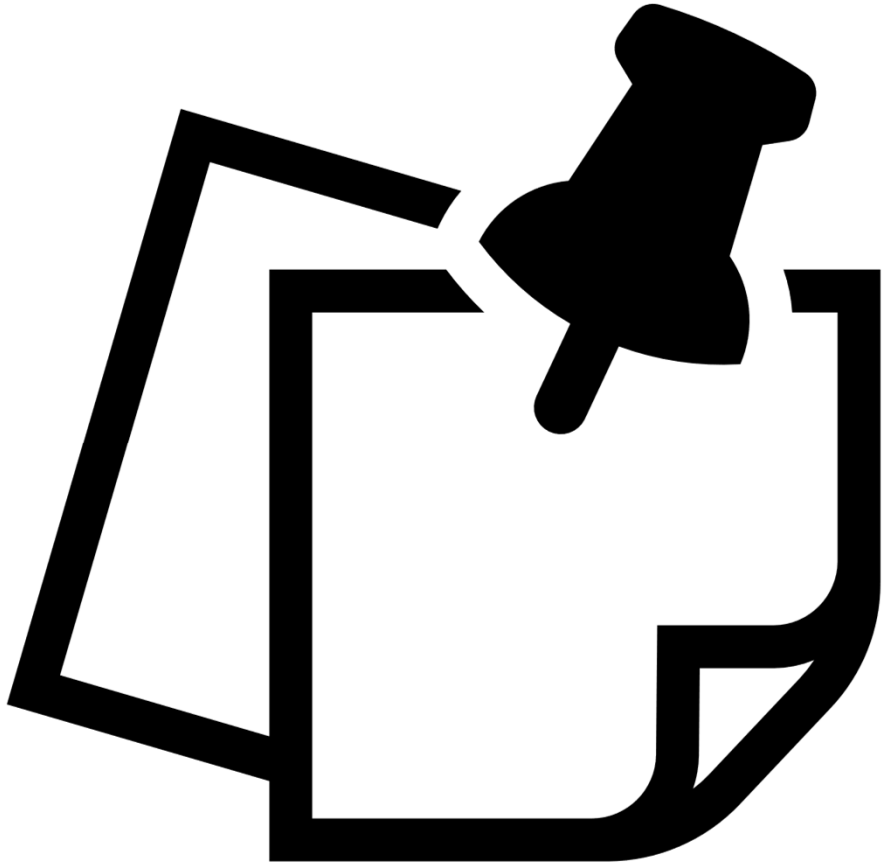
Ausmaß, indem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden.



Quelle: C. Witt (2010), nach ISO 9000

DEFINITION: *EFFIZIENZ*

Verhältnis zwischen erzieltem Ergebnis gegenüber den eingesetzten Mitteln.



Quelle: C. Witt (2010) nach ISO 9000

2.1

INTERNATIONALE HOCHSCHULE

DATENSCHUTZRECHTLICHE KONZEPTE

GRUNDSÄTZE DES DATENSCHUTZES

- **Datenschutz** ist in Deutschland und der EU ein **Grundrecht**, nämlich das **Recht auf informationelle Selbstbestimmung**.
  - Recht des Einzelnen, selbst über die **Erhebung** und die **Verwendung** der ihn persönlich betreffenden Daten zu bestimmen
  - jedem selbst überlassen, ob er Informationen über sich im Internet veröffentlicht oder nicht
  - Werden gegen seinen Willen solche Veröffentlichungen gemacht, kann er dagegen vorgehen, da sein Recht auf informationelle Selbstbestimmung verletzt wurde

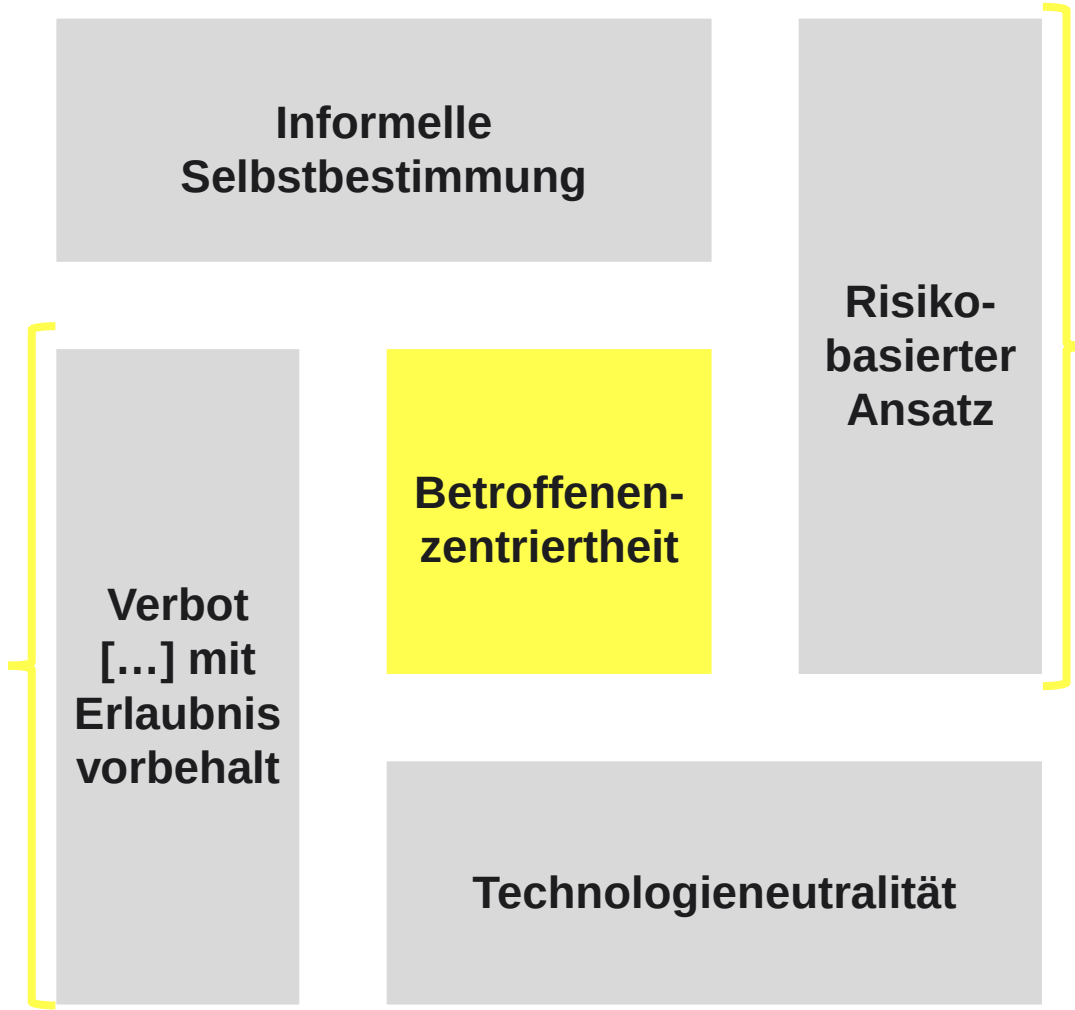
- **Hauptziel des Datenschutzes** ist demnach, das Recht des Einzelnen auf **informationelle Selbstbestimmung** zu garantieren
  - Bedeutet nicht, dass etwa jegliche Weitergabe von Daten über Personen verboten wird

- Gefährdung, die mit dem Datenschutzrecht geregelt werden soll, ist insbesondere diejenige, bei der Muster gebildet werden können → Gewinnung zusätzlicher Informationen

GRUNDSÄTZE DES DATENSCHUTZES - GRUNDPRINZIPIEN

INTERNATIONALE HOCHSCHULE

Das Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt in der DSGVO besagt, dass die **Verarbeitung solcher Daten grundsätzlich untersagt** ist, es sei denn, es liegt eine ausdrückliche gesetzliche Erlaubnis oder die ausdrückliche Einwilligung der betroffenen Person vor. Dieses Prinzip dient dem **Schutz der Privatsphäre und der Grundrechte von Personen**, indem es sicherstellt, dass ihre Daten nur unter bestimmten, klar definierten Bedingungen verarbeitet werden dürfen.



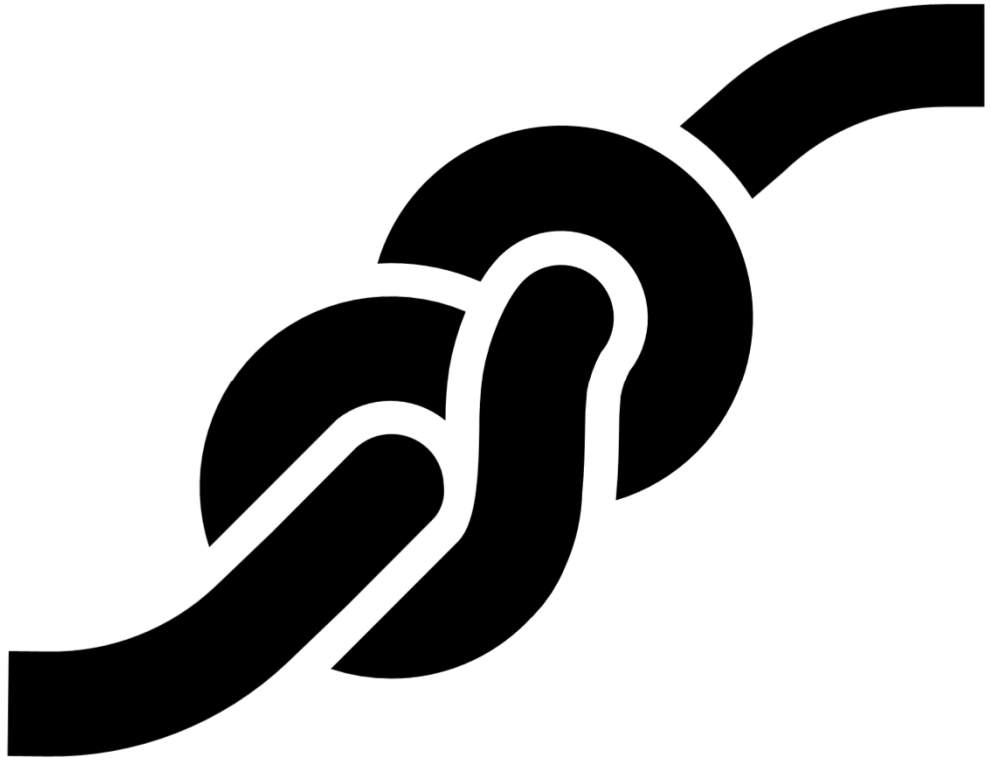
Der risikobasierte Ansatz in der DSGVO verlangt von Unternehmen und Organisationen, dass sie **Datenschutzmaßnahmen basierend auf dem Risiko implementieren**, das die Verarbeitung personenbezogener Daten für die Rechte und Freiheiten der betroffenen Personen darstellt. Dieser Ansatz erlaubt eine flexible und angemessene Anwendung von Datenschutzvorschriften, indem er sicherstellt, dass **Ressourcen und Bemühungen auf diejenigen Verarbeitungsaktivitäten fokussiert werden, die ein höheres Risiko für die betroffenen Personen darstellen**.

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *RECHTMÄßIGKEIT*

- **Rechtmäßigkeit:** Verarbeitung personenbezogener Daten muss auf einer gesetzlichen Grundlage oder der Einwilligung der betroffenen Person beruhen.
- **Verarbeitung nach Treu und Glauben:** Datenverarbeiter müssen in gutem Glauben handeln und die Interessen der betroffenen Personen respektieren.
- **Transparenz:** Die betroffene Person muss über die Verarbeitung ihrer Daten klar und verständlich informiert werden.
- **Informationspflicht:** Datenverarbeiter sind verpflichtet, betroffene Personen über ihre Rechte und die Verarbeitung ihrer Daten zu informieren.

Quelle: EU-DSGVO Artikel 5

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *ZWECKBINDUNG*



- **Zweckbindung:** Personendaten müssen für klar definierte und legitime Zwecke erhoben werden.
- **Keine inkompatible Weiterverarbeitung:** Daten dürfen nicht für Zwecke verarbeitet werden, die mit den ursprünglichen Zwecken unvereinbar sind.
- **Ausnahmen:** Weiterverarbeitung für Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke ist zulässig, wenn sie im öffentlichen Interesse liegt (gemäß Artikel 89 Absatz 1).
- **Schutzmechanismen:** Bei der Weiterverarbeitung sind geeignete Sicherheitsmaßnahmen und Garantien zum Schutz der betroffenen Personen erforderlich.
- **Verantwortung:** Datenverarbeiter müssen sicherstellen, dass die Zweckbindung eingehalten wird und die Verarbeitung der Daten im Einklang mit den ursprünglichen Zwecken steht.

Quelle: EU-DSGVO Artikel 5

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *ZWECKBINDUNG*

- **Datenminimierung:** Datenverarbeitung sollte nur in dem Umfang erfolgen, der für den festgelegten Zweck notwendig ist.
- **Angemessenheit:** Verarbeitete Daten sollten relevant und geeignet für den beabsichtigten Zweck sein.
- **Begrenzung:** Die Menge der erhobenen und verarbeiteten Daten sollte auf das notwendige Minimum reduziert werden.
- **Speicherdauer:** Personenbezogene Daten sollten nicht länger als für den Verarbeitungszweck erforderlich aufbewahrt werden.
- **Verantwortung:** Datenverarbeiter müssen sicherstellen, dass die Datenminimierung bei der Erhebung, Verarbeitung und Speicherung personenbezogener Daten eingehalten wird.

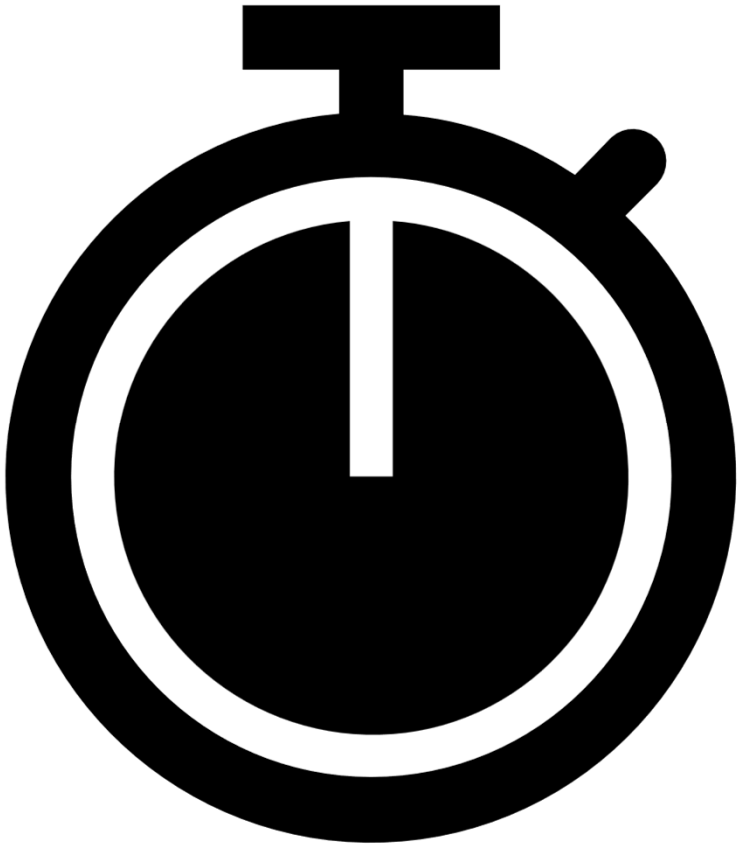
Quelle: EU-DSGVO Artikel 5

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *RICHTIGKEIT*

- **Richtigkeit:** Personenbezogene Daten müssen sachlich korrekt und aktuell sein.
- **Aktualisierung:** Datenverarbeiter sind verpflichtet, veraltete oder ungenaue Daten zu aktualisieren, wenn erforderlich.
- **Löschung/Berichtigung:** Unrichtige Daten müssen unverzüglich gelöscht oder berichtigt werden.
- **Verantwortung:** Datenverarbeiter müssen geeignete Maßnahmen ergreifen, um die Richtigkeit der verarbeiteten Daten sicherzustellen.
- **Betroffenenrechte:** Betroffene Personen haben das Recht auf Berichtigung unrichtiger Daten und auf Löschung ihrer personenbezogenen Daten, wenn entsprechende Voraussetzungen erfüllt sind.

Quelle: EU-DSGVO Artikel 5

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *SPEICHERBEGRENZUNG*



- **Speicherbegrenzung:** Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Verarbeitungszweck erforderlich ist.
- **Identifizierung:** Daten sollten in einer Form gespeichert werden, die eine Identifizierung der betroffenen Personen nur für die erforderliche Dauer ermöglicht.
- Längere Speicherung: Eine längere Speicherung ist zulässig, wenn die Daten für Archivzwecke, wissenschaftliche/historische Forschung oder statistische Zwecke im öffentlichen Interesse verwendet werden (gemäß Artikel 89 Absatz 1).
- **Umsetzung:** Datenverarbeiter müssen sicherstellen, dass die Speicherbegrenzung eingehalten wird.

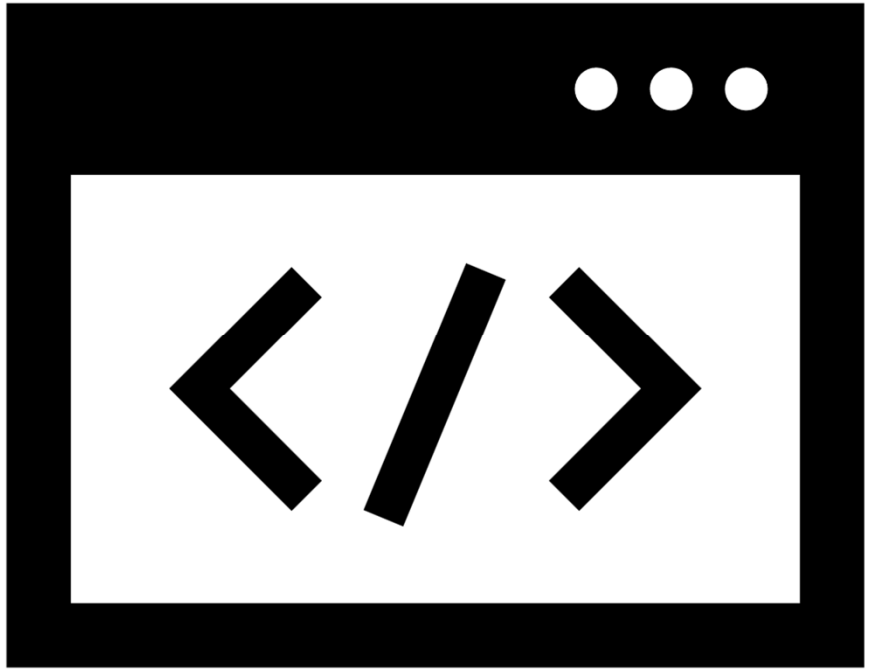
Quelle: EU-DSGVO Artikel 5

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *INTEGRITÄT UND VERTRAULICHKEIT*

- **Integrität und Vertraulichkeit:** Personenbezogene Daten müssen sicher und vor unbefugtem Zugriff oder Missbrauch geschützt verarbeitet werden.
- **Technische Maßnahmen:** Einsatz von geeigneten Technologien, z. B. Verschlüsselung und Firewall, um die Sicherheit der Daten zu gewährleisten.
- **Organisatorische Maßnahmen:** Implementierung von internen Richtlinien, Verfahren und Schulungen, um das Bewusstsein für Datenschutz zu fördern und den Schutz personenbezogener Daten sicherzustellen.
- **Schutz vor Verlust und Schädigung:** Datenverarbeiter müssen Vorkehrungen treffen, um unbeabsichtigten Verlust, Zerstörung oder Schädigung der personenbezogenen Daten zu verhindern.
- **Umsetzung:** Datenverarbeiter sind verpflichtet, die Integrität und Vertraulichkeit der verarbeiteten personenbezogenen Daten kontinuierlich zu überprüfen und aufrechtzuerhalten.

Quelle: EU-DSGVO Artikel 5

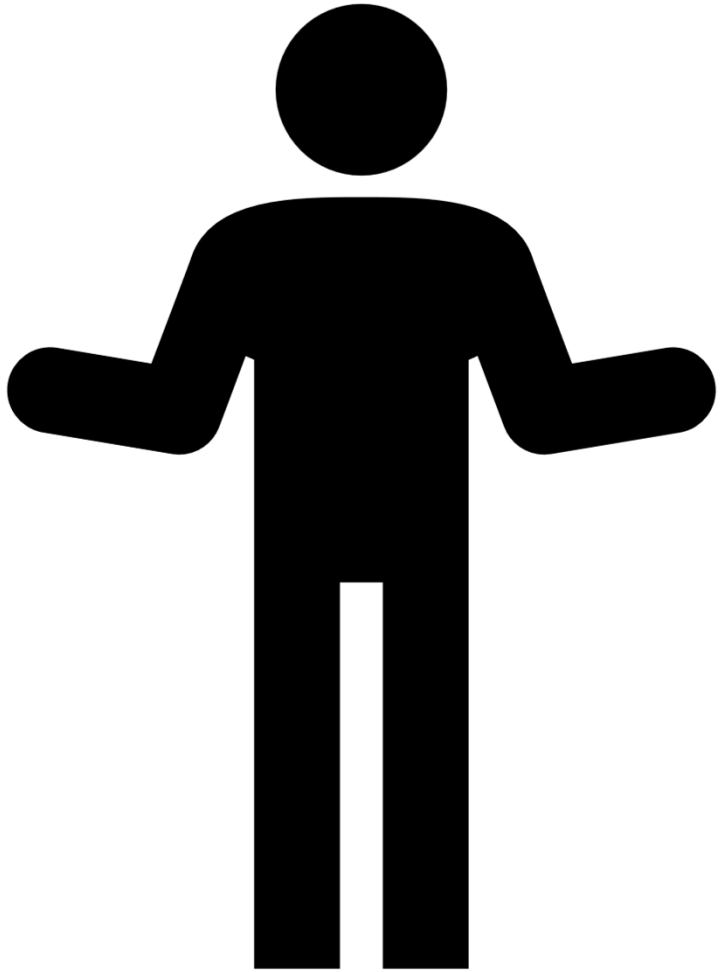
GRUNDSÄTZE DES DATENSCHUTZES
EXKURS *PRIVACY BY DESIGN*



1. Proaktiver und nicht reaktiver Datenschutz
2. Datenschutz als Standard
3. Datenschutz in die Technik einbetten
4. Vollständige Funktionalität – positives Nutzererlebnis
5. Datensicherheit über den gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz
7. Respekt vor der Privatsphäre der Nutzer

Quelle: EU-DSGVO Artikel 5

GRUNDSÄTZE DES DATENSCHUTZES
PRINZIP *RECHENSCHAFTSPFLICHT*



Quelle: EU-DSGVO Artikel 5

- **Rechenschaftspflicht:** Der Verantwortliche trägt die Verantwortung für die Einhaltung der Datenschutzprinzipien und muss deren Einhaltung nachweisen können.
- **Dokumentation:** Der Verantwortliche muss Datenschutzmaßnahmen und -verfahren dokumentieren, um die Einhaltung der DSGVO zu belegen.
- **Risikobewertung:** Durchführung von Datenschutz-Folgenabschätzungen, um Risiken in der Datenverarbeitung zu identifizieren und angemessene Schutzmaßnahmen zu ergreifen.
- **Mitarbeiterschulung:** Sicherstellen, dass alle Mitarbeiter über die Datenschutzanforderungen informiert sind und diese in der täglichen Arbeit einhalten.
- **Zusammenarbeit mit Datenschutzbehörden:** Der Verantwortliche muss bei Bedarf mit den zuständigen Datenschutzbehörden zusammenarbeiten und deren Anweisungen befolgen, um die Einhaltung der DSGVO nachzuweisen.

PRINZIPIEN DES DATENSCHUTZES

Datengeheimnis	Es ist untersagt, personenbezogene Daten unbefugt zu erheben oder zu verwenden
Datenvermeidung	Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben oder zu verwenden.
Erforderlichkeit	Erforderlich sind personenbezogene Daten nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann.
Interessenabwägung	Die berechtigten Interessen der erhebenden bzw. verwendenden Stelle sind immer gegenüber den schutzwürdigen Interessen Betroffener abzuwägen.
Schutzbedarf	Es sind technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der eingesetzten IT im Interesse des Schutzes des Persönlichkeitsrechtes zu gewährleisten.

Quelle: BDSG

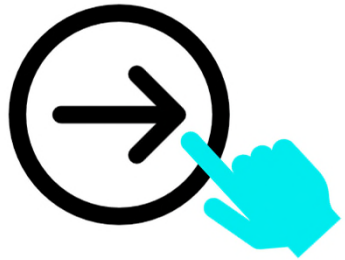
PRINZIPIEN DES DATENSCHUTZES

Selbstauskunft	Die Erhebung personenbezogener Daten muss – soweit möglich – beim Betroffenen erfolgen.
Transparenz	Es ist Pflicht, den Betroffenen (dessen Daten gespeichert werden) über die Daten, die Zweckbestimmung der Erhebung und Verwendung und die Identität der verantwortlichen Stelle zu informieren.
Verhältnismäßigkeit	Nicht mehr Personenbezogene Daten erheben oder verwenden als notwendig („Übermaßverbot“).
Zweckbindung	Bei jeder Erhebung oder Verwendung PBD ist zwingend ein hinreichend präziser Verwendungszweck festzulegen, von dem nur in wohl definierten Ausnahmefällen abgewichen werden kann.

Quelle: BDSG

DATENSCHUTZ

Übung: Prinzipien



(Password: DaSchu_ITS_24)

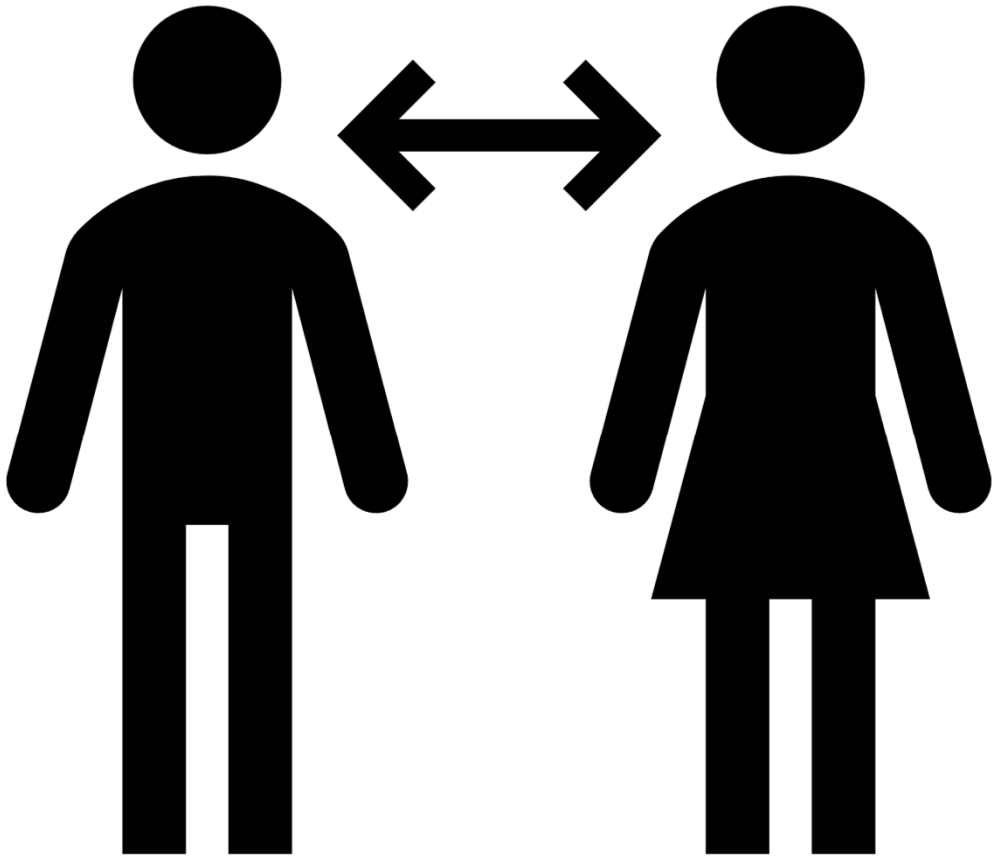
45 Minuten - Gruppenarbeit

1) Finden Sie in der Gruppe für jedes der genannten Datenschutzprinzipien mindestens ein konkretes Beispiel aus der täglichen Arbeit (bei Ihrem Praxispartner).

2) Entwickeln Sie in der Gruppe ein Konzept für eine mobile Anwendung, die den Datenschutz der Nutzerinnen und Nutzer sicherstellt. Die Anwendung soll einen Ortungsdienst (z.B. für Freunde oder Familienmitglieder) bieten, um den Aufenthaltsort der Nutzerinnen und Nutzer in Echtzeit zu verfolgen und sie mit anderen zu teilen.
Berücksichtigen Sie bei der Konzeption der Anwendung die sieben Grundprinzipien von Privacy by Design. Identifizieren Sie spezifische Maßnahmen und Funktionen, die in der Anwendung implementiert werden sollen, um die Privatsphäre der Nutzerinnen und Nutzer zu schützen.

3) Präsentieren Sie Ihr Konzept in einem kurzen Vortrag (5-7 Minuten) im Plenum und diskutieren Sie die Vor- und Nachteile der vorgeschlagenen Maßnahmen. (zufällige Gruppe)

BETROFFENENRECHTE
KOMMUNIKATION UND MODALITÄTEN



- **Transparenz:** Der Datenverantwortliche muss betroffene Personen klar und verständlich über die Verarbeitung ihrer personenbezogenen Daten informieren.
- **Informationspflicht:** Bereitstellung von Informationen über Verarbeitungszwecke, Empfänger, Speicherdauer und Betroffenenrechte gemäß Artikel 13 und 14 der DSGVO.
- **Kommunikation:** Schnelle und effektive Kommunikation mit betroffenen Personen bei Anfragen zur Ausübung ihrer Datenschutzrechte (z.B. Zugang, Berichtigung, Löschung).
- **Modalitäten:** Bereitstellung von einfachen und zugänglichen Mitteln für die betroffene Person, um ihre Rechte auszuüben, einschließlich elektronischer Formulare und Kontaktmöglichkeiten.
- **Kostenfreiheit:** Die Ausübung der Betroffenenrechte sollte in der Regel kostenlos sein, es sei denn, Anfragen sind offensichtlich unbegründet oder übermäßig häufig.

Quelle: EU-DSGVO Artikel 12

BETROFFENENRECHTE
INFORMATIONSPFLICHT (ERHEBUNG BEI BETROFFENER PERSON)

- **Informationspflicht:** Der Datenverantwortliche muss betroffene Personen aktiv informieren, wenn ihre personenbezogenen Daten erhoben werden.
- **Verarbeitungszwecke:** Die betroffene Person muss über die Zwecke der Datenverarbeitung und die Rechtsgrundlage für die Verarbeitung informiert werden.
- **Empfänger:** Informationen über Empfänger oder Kategorien von Empfängern, an die personenbezogene Daten weitergegeben werden, müssen bereitgestellt werden.
- **Speicherdauer:** Die betroffene Person muss über die vorgesehene Speicherdauer der personenbezogenen Daten oder die Kriterien für die Festlegung dieser Dauer informiert werden.
- **Betroffenenrechte:** Die betroffene Person muss über ihre Datenschutzrechte informiert werden, einschließlich des Rechts auf Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und das Recht auf Datenübertragbarkeit.

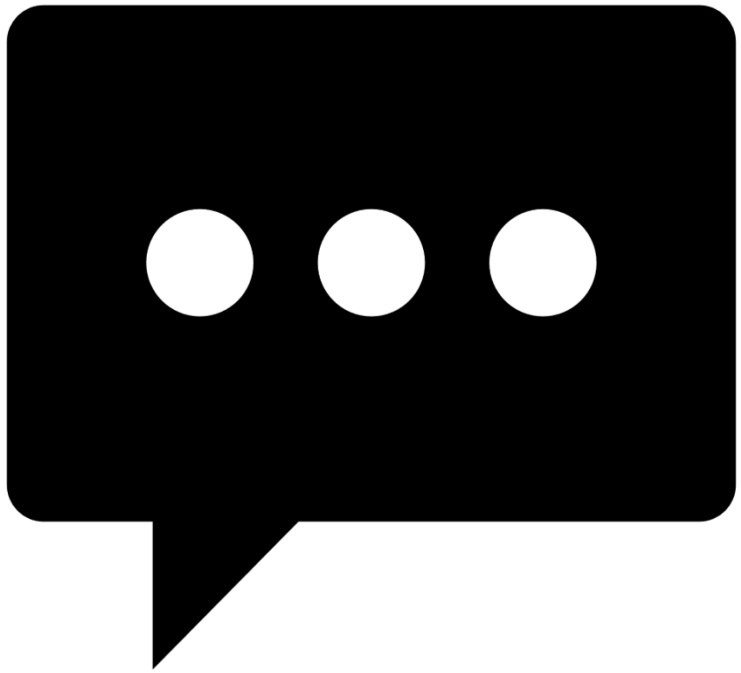
Quelle: EU-DSGVO Artikel 13

BETROFFENENRECHTE *INFORMATIONSPFLICHT (ERHEBUNG BEI NICHT-BETROFFENER PERSON)*

- **Informationspflicht:** Der Verantwortliche muss betroffene Personen informieren, wenn personenbezogene Daten nicht direkt von ihnen erhoben werden, sondern aus anderen Quellen stammen.
- **Informationsquellen:** Die betroffene Person muss über die Herkunft der Daten und, wenn möglich, die genaue Informationsquelle informiert werden.
- **Verarbeitungszwecke und Rechtsgrundlage:** Die betroffene Person muss über die Zwecke der Datenverarbeitung und die Rechtsgrundlage für die Verarbeitung informiert werden.
- **Zeit. der Information:** Die betroffene Person sollte innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach der Erhebung der Daten, informiert werden.
- **Ausnahmen:** In bestimmten Fällen, wie z.B. wenn die Informationsbereitstellung unmöglich oder unverhältnismäßig aufwendig ist, kann die Informationspflicht entfallen oder eingeschränkt sein.

Quelle: EU-DSGVO Artikel 14

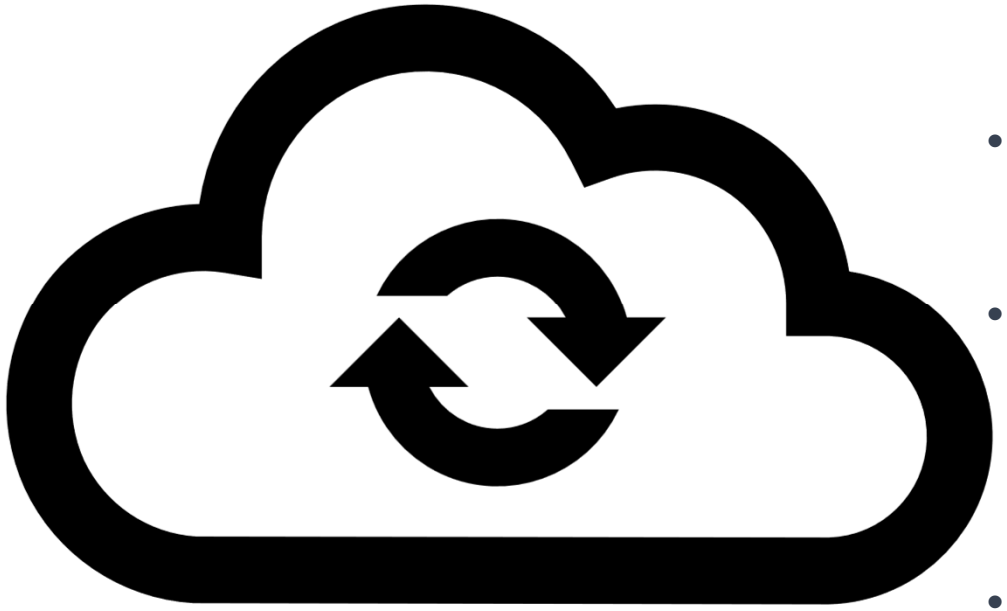
BETROFFENENRECHTE
AUSKUNFTSRECHT DER BETROFFENEN PERSON



- **Auskunftsrecht:** Betroffene Personen haben das Recht, von dem Verantwortlichen eine Bestätigung darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden.
- **Zugang zu Informationen:** Bei einer Verarbeitung haben betroffene Personen das Recht, Zugang zu ihren personenbezogenen Daten und Informationen über die Verarbeitungszwecke, Empfänger und Speicherdauer zu erhalten.
- **Recht auf Kopie:** Betroffene Personen haben das Recht, eine Kopie der verarbeiteten personenbezogenen Daten zu erhalten, solange dies die Rechte und Freiheiten anderer nicht beeinträchtigt.
- **Reaktionszeit:** Der Verantwortliche muss betroffenen Personen innerhalb eines Monats nach Eingang des Antrags auf Auskunft antworten, wobei diese Frist unter bestimmten Umständen verlängert werden kann.
- **Beschwerderecht:** Der Verantwortliche muss die betroffene Person über das Beschwerderecht bei einer Aufsichtsbehörde informieren.

Quelle: EU-DSGVO Artikel 15

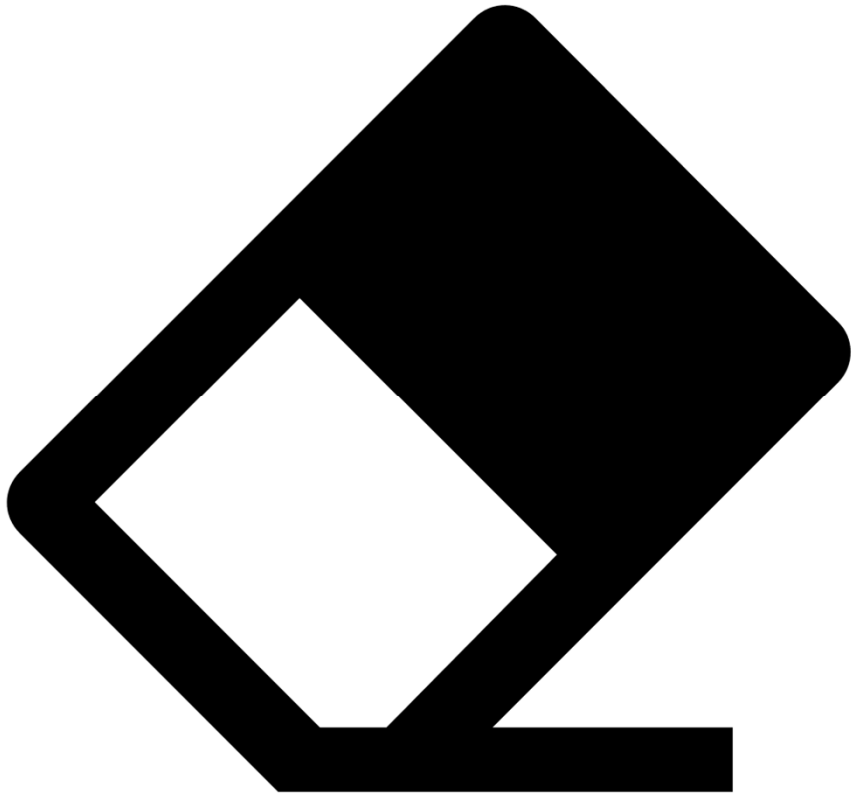
BETROFFENENRECHTE
RECHT AUF BERICHTIGUNG



- **Recht auf Berichtigung:** Betroffene Personen haben das Recht, von dem Datenverantwortlichen die Berichtigung unrichtiger oder unvollständiger personenbezogener Daten zu verlangen.
- **Unverzügliche Berichtigung:** Der Verantwortliche muss unrichtige oder unvollständige Daten unverzüglich berichtigen, sobald er von der Unrichtigkeit oder Unvollständigkeit Kenntnis erlangt.
- **Ergänzung fehlender Daten:** Betroffene Personen können die Ergänzung unvollständiger Daten verlangen, auch durch eine ergänzende Erklärung.
- **Mitteilung an Empfänger:** Wenn personenbezogene Daten offengelegt wurden, muss der Verantwortliche die Berichtigung in der Regel auch den Empfängern der Daten mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.
- **Reaktionszeit:** Der Verantwortliche muss betroffenen Personen innerhalb eines Monats nach Eingang des Antrags auf Berichtigung antworten, wobei diese Frist unter bestimmten Umständen verlängert werden kann.

Quelle: EU-DSGVO Artikel 16 &19

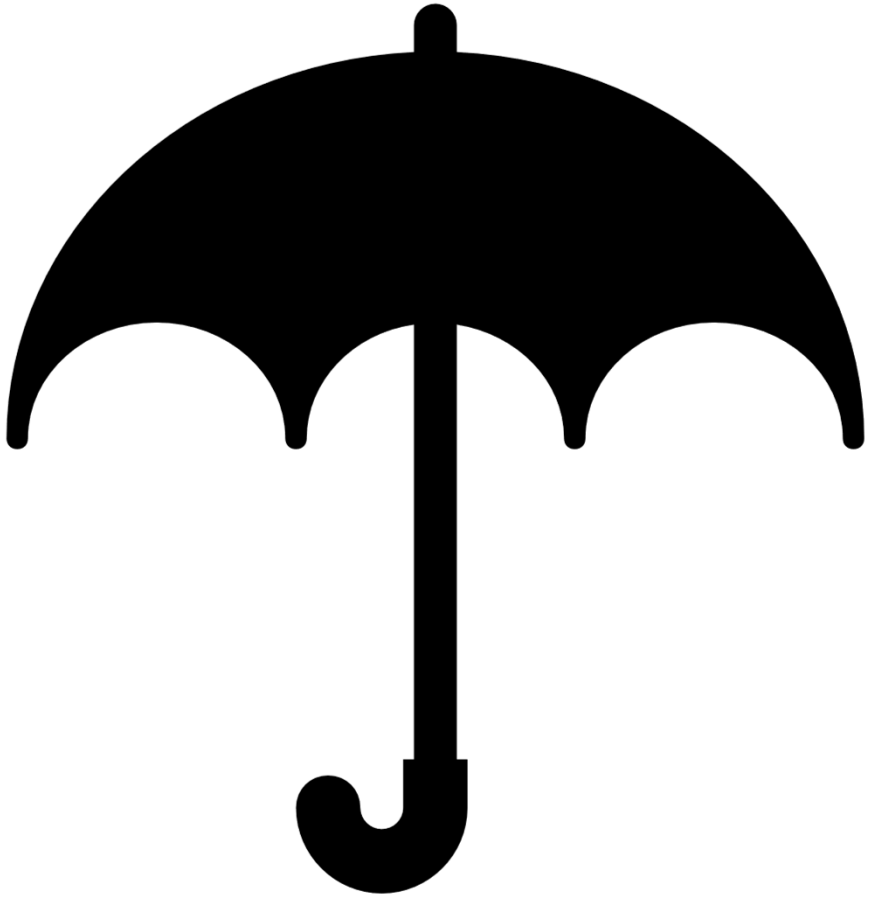
BETROFFENENRECHTE
RECHT AUF VERGESSENWERDEN



- **Recht auf Löschung:** Betroffene Personen haben das Recht, von dem Datenverantwortlichen die Löschung ihrer personenbezogenen Daten zu verlangen, wenn bestimmte Voraussetzungen erfüllt sind.
- **Löschungsgründe:** Gründe für eine Löschung können sein: Daten sind für den ursprünglichen Zweck nicht mehr erforderlich, Widerruf der Einwilligung, berechtigter Widerspruch, unrechtmäßige Verarbeitung oder gesetzliche Löschungspflichten.
- **Recht auf Vergessenwerden:** Bei öffentlich gemachten Daten muss der Verantwortliche angemessene Maßnahmen ergreifen, um andere Verantwortliche zu informieren, dass die betroffene Person die Löschung aller Links, Kopien oder Replikationen ihrer Daten verlangt hat.
- **Ausnahmen:** Das Recht auf Löschung besteht nicht, wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrung öffentlicher Interessen (z.B. Archivierung, Forschung) erforderlich ist.
- **Reaktionszeit:** Der Verantwortliche muss betroffenen Personen innerhalb eines Monats nach Eingang des Antrags auf Löschung antworten, wobei diese Frist unter bestimmten Umständen verlängert werden kann.

Quelle: EU-DSGVO Artikel 17 & 19

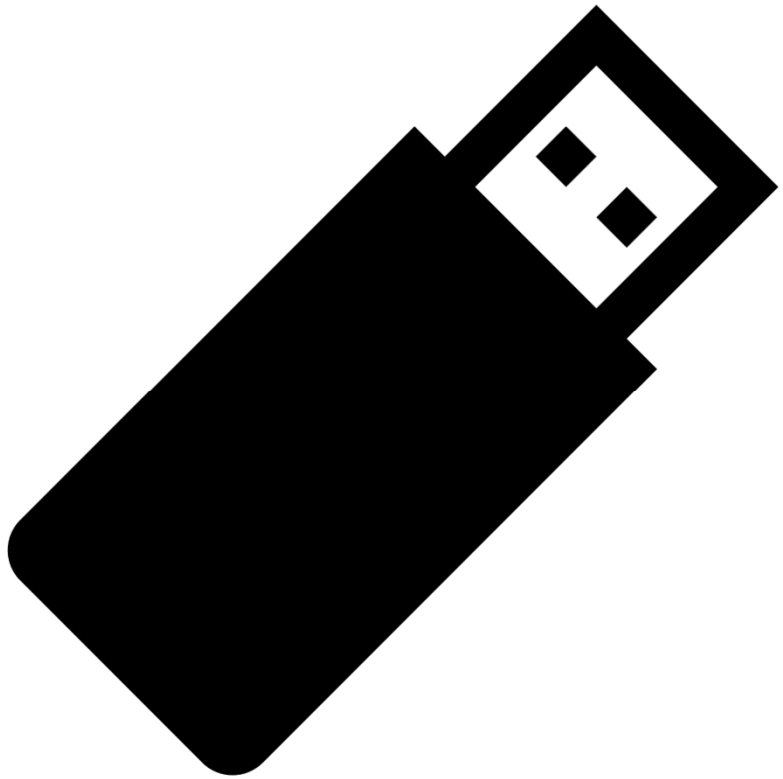
BETROFFENENRECHTE
RECHT AUF EINSCHRÄNKUNG DER VERARBEITUNG



- **Recht auf Einschränkung:** Betroffene Personen haben das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen, wenn bestimmte Bedingungen erfüllt sind.
- **Einschränkungsgründe:** E. g. Überprüfung der Richtigkeit der Daten, unrechtmäßige Verarbeitung mit Ablehnung der Löschung, Speicherung der Daten für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder Prüfung eines Widerspruchs gegen die Verarbeitung.
- **Eingeschränkte Verarbeitung:** Bei eingeschränkter Verarbeitung dürfen personenbezogene Daten nur mit Einwilligung der betroffenen Person, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz der Rechte anderer Personen oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden.
- **Mitteilung an Empfänger:** Der Verantwortliche muss die Empfänger der Daten über die Einschränkung der Verarbeitung informieren, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.
- **Reaktionszeit:** Der Datenverantwortliche muss betroffenen Personen innerhalb eines Monats nach Eingang des Antrags auf Einschränkung der Verarbeitung antworten, wobei diese Frist unter bestimmten Umständen verlängert werden kann.

Quelle: EU-DSGVO Artikel 18 & 19

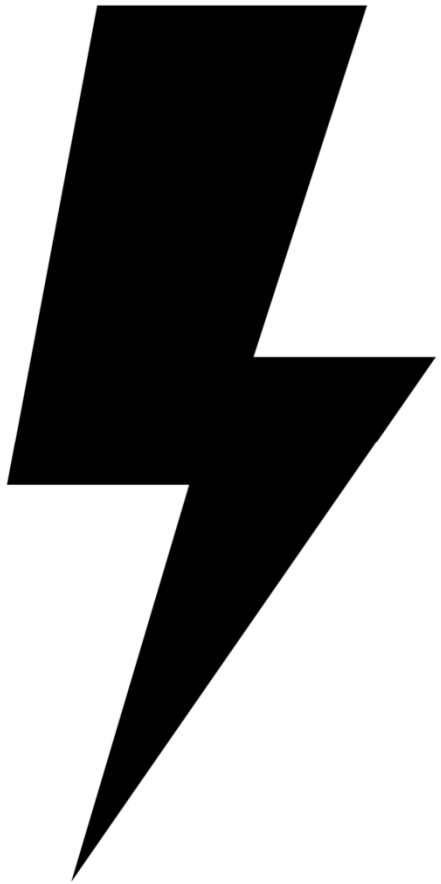
BETROFFENENRECHTE
RECHT AUF DATENÜBERTRAGBARKEIT



- **Recht auf Datenübertragbarkeit:** Betroffene Personen haben das Recht, ihre personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
- **Direkte Übermittlung:** Betroffene Personen haben das Recht, die direkte Übermittlung ihrer Daten von einem Verantwortlichen zu einem anderen zu verlangen, sofern dies technisch machbar ist.
- **Anwendbarkeit:** Dieses Recht gilt nur, wenn die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren durchgeführt wird.
- **Keine Beeinträchtigung:** Die Ausübung des Rechts auf Datenübertragbarkeit darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen, insbesondere nicht das Schutzbedürfnis der personenbezogenen Daten anderer betroffener Personen.
- **Reaktionszeit:** Der Verantwortliche muss betroffenen Personen innerhalb eines Monats nach Eingang des Antrags auf Datenübertragbarkeit antworten, wobei diese Frist unter bestimmten Umständen verlängert werden kann.

Quelle: EU-DSGVO Artikel 20

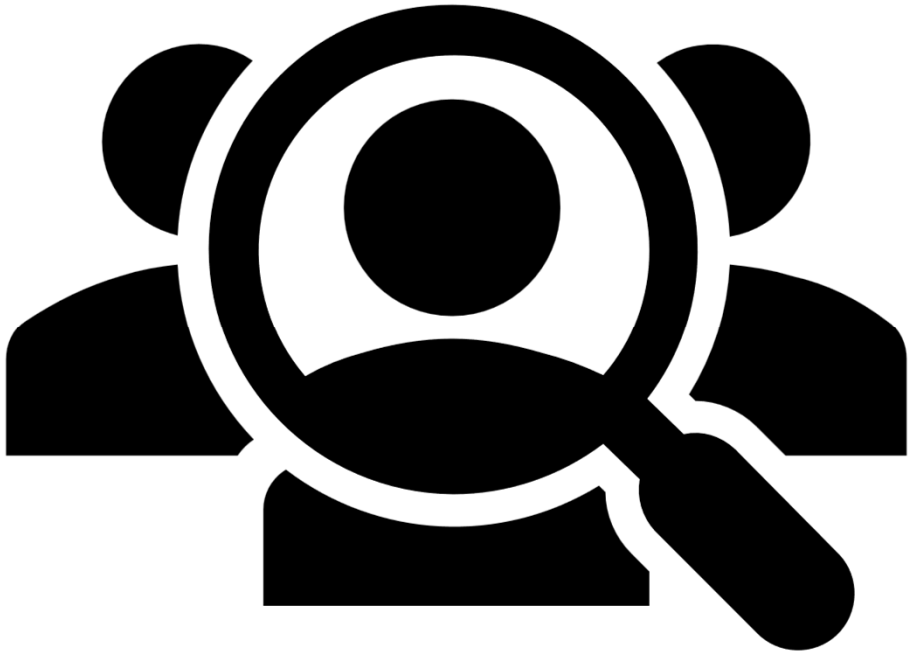
BETROFFENENRECHTE
WIDERSPRUCHSRECHT



- **Widerspruchsrecht:** Betroffene Personen haben das Recht, jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen, wenn diese aufgrund von berechtigten Interessen des Verantwortlichen oder eines Dritten oder im Rahmen einer Aufgabe im öffentlichen Interesse erfolgt.
- **Direktmarketing:** Bei Verarbeitung für Zwecke des Direktmarketings können betroffene Personen jederzeit Widerspruch einlegen, woraufhin ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet werden dürfen.
- **Begründung:** Der Widerspruch muss auf Gründe gestützt werden, die sich auf die besondere Situation der betroffenen Person beziehen, es sei denn, es handelt sich um Direktmarketing.
- **Prüfung des Widerspruchs:** Der Verantwortliche muss den Widerspruch prüfen und die Verarbeitung einstellen, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- **Unterrichtungspflicht:** Betroffene Personen müssen bei der ersten Kommunikation mit dem Verantwortlichen ausdrücklich auf ihr Widerspruchsrecht hingewiesen werden und dieser Hinweis muss verständlich und von anderen Informationen getrennt erfolgen.

Quelle: EU-DSGVO Artikel 21

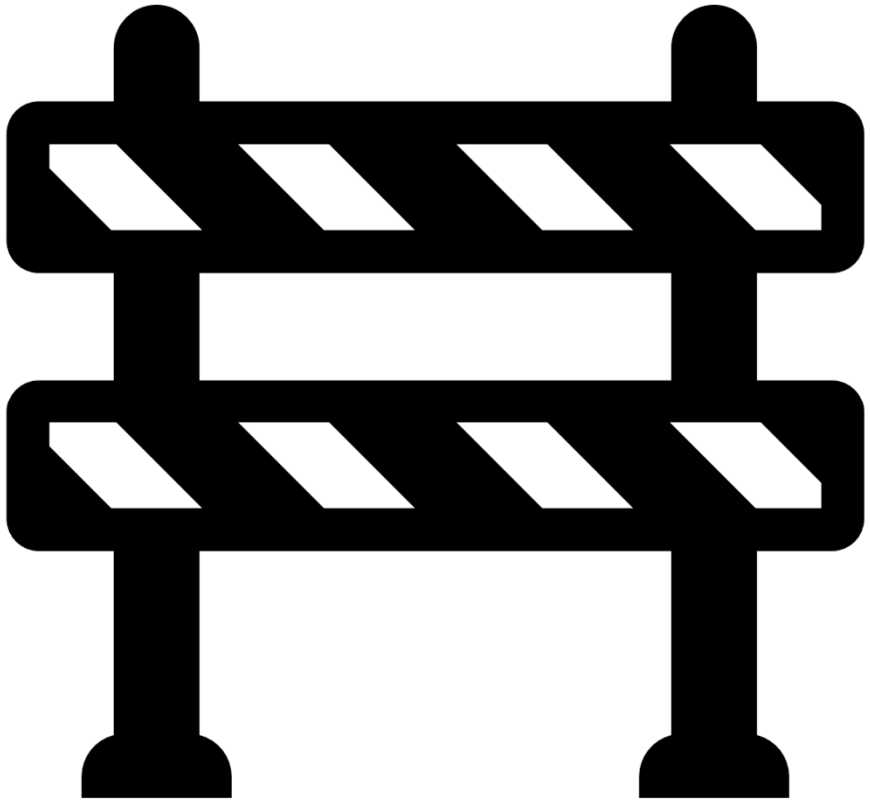
BETROFFENENRECHTE - *AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL EINSCHLIEßLICH PROFILING*



- **Automatisierte Entscheidungen:** Betroffene Personen haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
- **Ausnahmen:** Automatisierte Entscheidungen sind zulässig, wenn sie für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich sind, aufgrund von rechtlichen Vorschriften zulässig sind, oder wenn die betroffene Person ausdrücklich eingewilligt hat.
- **Schutzmaßnahmen:** Bei zulässigen automatisierten Entscheidungen müssen angemessene Schutzmaßnahmen getroffen werden, um die Rechte, Freiheiten und berechtigten Interessen der betroffenen Personen zu wahren, einschließlich des Rechts auf menschliches Eingreifen seitens des Verantwortlichen, des Rechts, den eigenen Stand. darzulegen, und des Rechts, die Entscheidung anzufechten.
- **Verbot diskriminierender Entscheidungen:** Automatisierte Entscheidungen dürfen keine Diskriminierung aufgrund von besonderen Kategorien personenbezogener Daten, bewirken, es sei denn, dies ist durch Rechtsvorschriften zugelassen und angemessene Schutzmaßnahmen wurden getroffen.

Quelle: EU-DSGVO Artikel 22

BETROFFENENRECHTE
BESCHRÄNKUNGEN



- **Beschränkungen:** Mitgliedstaaten können durch Rechtsvorschriften Einschränkungen der Datenschutzrechte und -pflichten vorsehen, wenn diese zur Wahrung wichtiger öffentlicher oder privater Interessen erforderlich sind.
- **Schutzbedürftige Interessen:** Zu den schutzwürdigen Interessen zählen nationale Sicherheit, Landesverteidigung, öffentliche Sicherheit, Strafverfolgung, Schutz vor schwerwiegenden Bedrohungen, wichtige wirtschaftliche oder finanzielle Interessen, Schutz der Unabhängigkeit der Justiz und Rechtsdurchsetzung sowie Schutz von Rechten und Freiheiten anderer Personen.
- **Verhältnismäßigkeit:** Jede Einschränkung der Datenschutzrechte und -pflichten muss verhältnismäßig und notwendig sein, um die schutzbedürftigen Interessen zu wahren, und darf nicht über das erforderliche Maß hinausgehen.
- **Verfahrensgarantien:** Die Rechtsvorschriften müssen angemessene Verfahrens- und Rechtsschutzgarantien gewährleisten, um die Rechte der betroffenen Personen, insbesondere das Recht auf wirksamen gerichtlichen Rechtsschutz, zu schützen.

Quelle: EU-DSGVO Artikel 23

DATENSCHUTZ

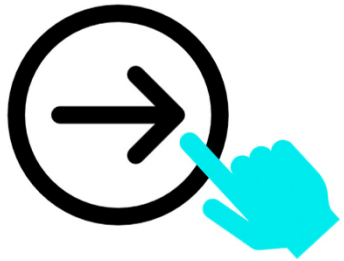
Übung: Betroffenenrechte

20 Minuten - Gruppenarbeit

1) Wählen Sie ein Unternehmen Ihrer Wahl (e.g. Ihren Praxispartner), beschreiben Sie einen typischen Betroffenen und recherchieren, wie dieser seine Rechte durchsetzen kann.

2) Visualisieren Sie Ihre Ergebnisse farblich in Miro (rot = keine Information vorhanden oder fehlerhaft, gelb = keine „überzeugende“ Information, grün = kommunizierte Möglichkeit transparent und passend).

3) Geben Sie an wie oft Sie in den letzten fünf Jahren (bewusst) von Ihren Betroffenenrechten Gebrauch gemacht haben.



(Password: DaSchu_ITS_24)

“Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit **Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden**, die sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.“

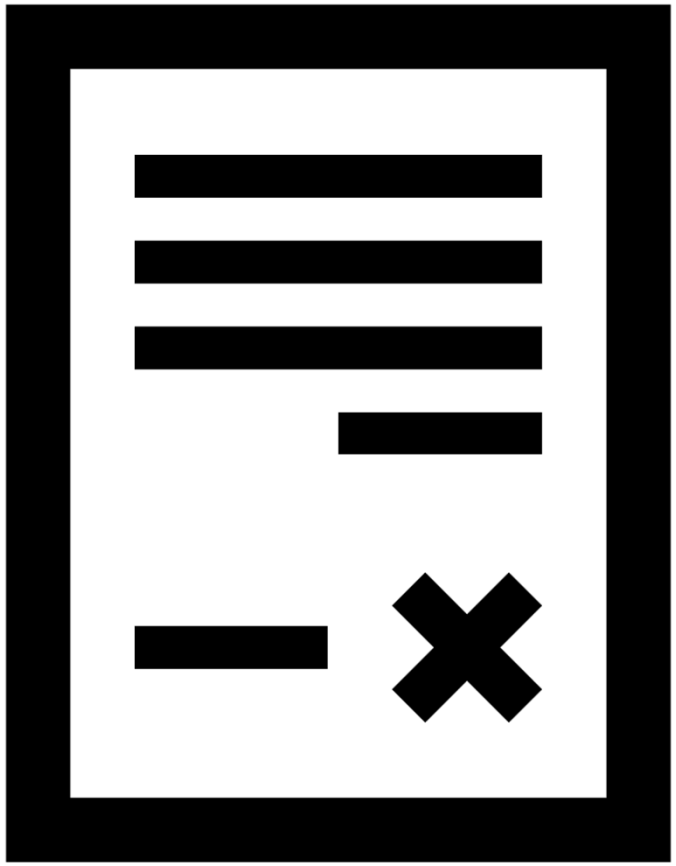
- Erwägungsgrund 40 EU-DSGVO

RECHTMÄßIGKEIT DER VERARBEITUNG
EINWILLIGUNG

- **Nachweis der Einwilligung:** Verantwortliche müssen nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- **Einwilligungserklärung:** Bei schriftlichen Erklärungen muss das Ersuchen um Einwilligung klar von anderen Sachverhalten getrennt, verständlich und leicht zugänglich sein. Unzulässige Teile der Erklärung sind nicht bindend.
- **Widerrufsrecht:** Betroffene Personen haben das Recht, ihre Einwilligung jederzeit zu widerrufen, ohne die Rechtmäßigkeit der vorherigen Verarbeitung zu beeinträchtigen. Sie müssen über dieses Recht informiert werden und der Widerruf soll so einfach wie die Erteilung der Einwilligung sein.
- **Freiwilligkeit der Einwilligung:** Bei der Beurteilung der Freiwilligkeit muss berücksichtigt werden, ob die Einwilligung zur Verarbeitung von Daten als Bedingung für einen Vertrag oder eine Dienstleistung erforderlich ist, obwohl sie nicht notwendig für die Erfüllung des Vertrags sind.
- **Schutz der betroffenen Person:** Einwilligungen müssen freiwillig, informiert und unmissverständlich erfolgen, um die Rechte der betroffenen Personen zu schützen und die datenschutzrechtlichen Anforderungen zu erfüllen.

Quelle: EU-DSGVO Artikel 7

RECHTMÄßIGKEIT DER VERARBEITUNG
VERTRAG ODER VORVERTRAGLICHE MAßNAHMEN



- **Beschränkungen:** Gilt nur, wenn die betroffene Person Vertragspartner ist. Insbesondere findet die Regelung keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen von B2B-Verträgen.
- **Vorvertragliche Maßnahmen:** Vorvertragliche Maßnahmen müssen auf Antrag der betroffenen Person erfolgt sein. Hierzu gehören beispielsweise Zusendung von Angebotsschreiben, Antrag auf Ratenkauf, oder auch Bewerbungsverfahren.

Quelle: EU-DSGVO Artikel 6

RECHTMÄßIGKEIT DER VERARBEITUNG
RECHTLICHE VERPFLICHTUNG

- **Beschränkungen:** die Regelung umfasst rechtliche Verpflichtungen im Sinne einer gesetzlichen Vorgabe jedoch nicht für vertraglich bedingte Verpflichtungen.
- **Anforderungen:** Es muss eine Prüfung für jede Rechtsnorm durchgeführt werden:
  - Die Rechtsnorm muss tatsächlich die Verpflichtung beinhalten, dass die Verarbeitung für die Erfüllung der Verpflichtung erforderlich ist.
  - Aufbewahrungsfristen müssen sich aus der Rechtsnorm ableiten lassen.
- **Beispiele:**
  - Aufbewahrungspflichten von Geschäftsunterlagen
  - Aufbewahrungspflichten im Gesundheits- und Sozialwesen
  - Meldepflichten im Zusammenhang mit Infektionen und Erkrankungen
  - Meldepflichten von Unterkünften

Quelle: EU-DSGVO Artikel 6

RECHTMÄßIGKEIT DER VERARBEITUNG
LEBENSWICHTIGE INTERESSEN

- **Beschränkungen:** was eine Datenverarbeitung ist zulässig Komma wenn sie dem Schutz lebenswichtiger Interessen der von der Verarbeitung betroffenen oder einer anderen natürlichen Person dient.
- **Erforderlichkeit:** Die Verarbeitung ist für den Schutz tatsächlich erforderlich sein.
- **Praktische Bedeutung:** dieser Erlaubnistatbestand hat in der Praxis eine untergeordnete Bedeutung da die Hürde der lebenswichtigen Interessen hoch ist und in der Regel personenbezogene Daten besonderer Art in diesem Falle Gesundheitsdaten betroffen sind. Für Gesundheitsdaten gelten nach der DSGVO gesonderte Erlaubnistatbestände (vgl. DSGVO Art. 9 Abs. 2).

Quelle: EU-DSGVO Artikel 6

RECHTMÄßIGKEIT DER VERARBEITUNG -*ÖFFENTLICHES INTERESSE ODER AUSÜBUNG ÖFFENTLICHER GEWALT*

- **Anwendung:** Zulässig, wenn sie zur Erfüllung einer öffentlichen Aufgabe oder zur Ausübung öffentlicher Gewalt erforderlich ist, die dem Verantwortlichen übertragen wurde.
- **Legitimation von Ämtern und Behörden:** Die Regelung dient der Legitimation der Arbeit von Ämtern und Behörden.
- **Rechtsgrundlage:** Erforderlich nach Unionsrecht oder dem Recht der Mitgliedstaaten gemäß Artikel 6 Absatz 3 DSGVO.
- **Keine generelle Berufung auf berechtigte Interessen:** Behörden können sich bei der Erfüllung ihrer Aufgaben nicht auf berechtigte Interessen berufen, da eine entsprechende Rechtsgrundlage erforderlich ist.

Quelle: EU-DSGVO Artikel 6

RECHTMÄßIGKEIT DER VERARBEITUNG - *BERECHTIGTES INTERESSE DES VERANTWORTLICHEN ODER EINES DRITTEN*

- **Beschränkungen:** Da betroffene Personen keine Dritte sein können, ist eine Verarbeitung auf Grundlage des mutmaßlichen Interesses der betroffenen Person hiermit nicht abgebildet.
- **Intressensidentifikation:** Zur Anwendung dieser Rechtsgrundlage muss das berechtigte Interesse identifiziert sein.
- **Interessenabwägung:** Im Rahmen der Anwendung dieser Rechtsgrundlage muss eine allgemeine und dokumentierte Interessenabwägung stattgefunden haben.
- **Informationspflicht:** Die berechtigten Interessen müssen im Rahmen der Informationspflichten angegeben werden.
- **Widerspruchsrecht:** Die die betroffene Person besitzt ein Widerspruchsrecht. Im Rahmen eines tatsächlichen Widerspruchs muss eine für die einzelne betroffene Person spezifische Interessenabwägung durchgeführt werden.

Quelle: EU-DSGVO Artikel 6

RECHTMÄßIGKEIT DER VERARBEITUNG

Einführungsbeispiel

- Eine Frau wehrt sich gegen die **Absage einer Sicherheitsfirma** wegen fehlender charakterlicher Eignung, die mit Verweis auf anonym zugespielte Bilder und Texte aus einem Internetforum begründet wurde.
- In dem Internetforum beschrieb die Frau, dass sie sich regelmäßig an Glücksspielen beteiligt, teilweise auch um große Summen. Die Frau erwähnte in diesem Internetforum unzutreffender Weise auch, dass sie bereits Mitarbeiterin der Sicherheitsfirma sei.
- Wurde der Frau zu Unrecht abgesagt?

- Ein Unternehmen speichert den gesamten E-Mail-Verkehr mit seinen Kunden im Rahmen der Bearbeitung der Bestellungen. Er wird später von einem Kunden wegen fehlerhafter Lieferung verklagt. Das Unternehmen legt den E-Mail-Verkehr mit diesem Kunden im Prozess zu seiner Verteidigung vor.

Quelle: R. Kneuper (2021)

RECHTMÄßIGKEIT DER VERARBEITUNG

Einführungsbeispiel - Bewertung

- Der Frau wird zu Recht abgesagt:
  - Zum einen hat nämlich die Sicherheitsfirma ein überwiegendes Interesse daran, die charakterliche Eignung von Bewerbern genau zu kennen.
  - Zum anderen hat die Frau die verwendeten Informationen selbst preisgegeben. Dass sie dabei auch noch unwahre Angaben gemacht hat, unterstreicht nur ihre mangelnde charakterliche Eignung.

- Auch darf das Unternehmen den E-Mail-Verkehr zu seiner Entlastung im Prozess vorlegen, da es sich nur so gegen den Vorwurf der falschen Lieferung wehren kann.

Quelle: R. Kneuper (2021)

RECHTMÄßIGKEIT DER VERARBEITUNG

Optionale Übung

1) Bildet Gruppen von 3-4 Personen und bearbeitet gemeinsam die folgende Fallstudie. Diskutiert und analysiert die Rechtmäßigkeit der Datenverarbeitung gemäß der DSGVO und identifiziert mögliche Verstöße oder Verbesserungspotenziale.

2) Fallstudie: Ein lokales Fitnessstudio möchte seinen Mitgliedern personalisierte Trainingspläne und Ernährungsempfehlungen anbieten. Dafür erhebt das Fitnessstudio folgende personenbezogene Daten von seinen Mitgliedern:

- Name, Adresse, Geburtsdatum, Geschlecht
- Größe, Gewicht, Körperfettanteil
- Trainingsziele (z.B. Gewichtsverlust, Muskelaufbau)
- Aktuelle körperliche Beschwerden oder Verletzungen
- Allergien und Unverträglichkeiten
- Fotos zur Dokumentation des Fortschritts

Die Mitglieder werden um ihre Einwilligung gebeten und ihnen wird erklärt, dass die erhobenen Daten ausschließlich zur Erstellung der personalisierten Trainingspläne und Ernährungsempfehlungen verwendet werden. Die Daten werden in einer Datenbank gespeichert, auf die nur autorisierte Trainer Zugriff haben.

3) Präsentiert eure Ergebnisse anschließend in der Gesamtgruppe und diskutiert gemeinsam, welche Maßnahmen das Fitnessstudio ergreifen sollte, um die Rechtmäßigkeit der Datenverarbeitung nach DSGVO sicherzustellen.

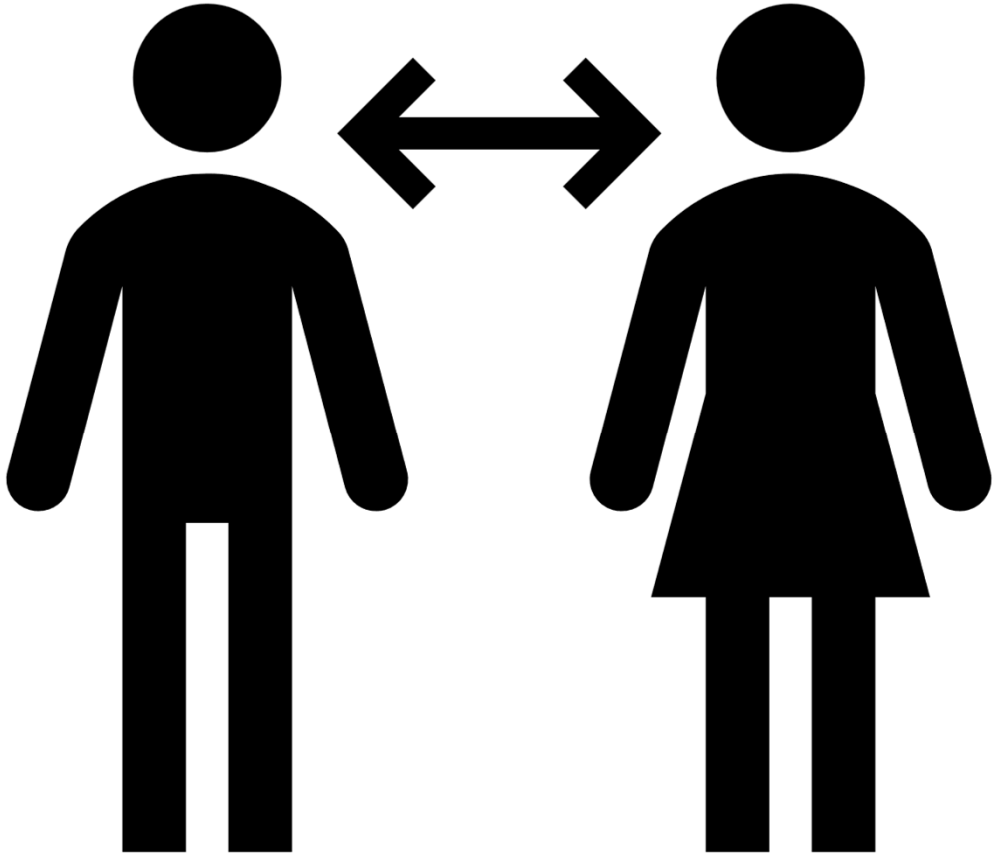
RECHTMÄßIGKEIT DER VERARBEITUNG

Übung - Diskussionspunkte

Diskussionspunkte:

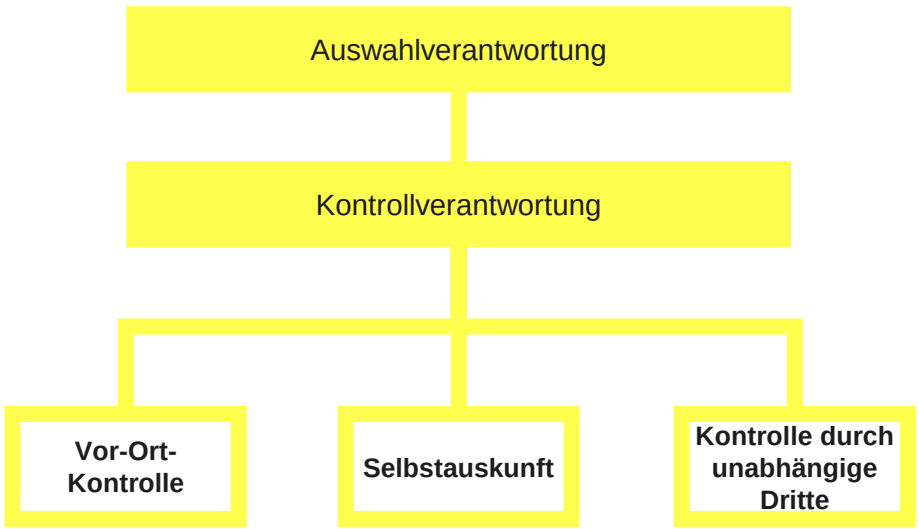
- Welche Rechtsgrundlagen könnten für die Datenverarbeitung in diesem Fall relevant sein? (z.B. Einwilligung, Vertragserfüllung)
- Wurde der Grundsatz der Datenminimierung beachtet? Gibt es Daten, die nicht notwendig für den angegebenen Zweck sind?
- Wurden die Grundsätze der Transparenz und Informationspflicht eingehalten? Wie könnte das Fitnessstudio die Mitglieder besser informieren?
- Wie könnte das Fitnessstudio sicherstellen, dass die Mitglieder ihre Rechte wahrnehmen können, z.B. Widerruf der Einwilligung, Auskunftsrecht, Berichtigung, Löschung?
- Welche technischen und organisatorischen Maßnahmen könnten das Fitnessstudio ergreifen, um die Integrität und Vertraulichkeit der personenbezogenen Daten zu gewährleisten?

ARBEITSTEILIGE VERARBEITUNG
ARTEN



- **Übermittlung zwischen (eigenständig) Verantwortlichen:** was jeder Verantwortliche legt die Zwecke der jeweiligen Datenvereinbarung frei fest und trägt die Hauptverantwortung für die Einhaltung der DSGVO. Die Datenverarbeitung erfolgt jeweils auf eigener Rechtsgrundlage
- **Gemeinsam Verantwortliche:** Nach Artikel 26 DSGVO ist eine gemeinsame Verantwortlichkeit von zwei oder mehr Verantwortlichen die gemeinsam die Zwecke und Mittel der Verarbeitung festlegen möglich. Diese Form der gemeinsamen Verantwortlichkeit wird auch als **Joint Controllership** bezeichnet. Die Beteiligten müssen in einer Vereinbarung festlegen, wer von ihnen welche Verpflichtungen aus der DSGVO erfüllt.
- **Auftragsverarbeiter:** *Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. (Art. 28 DSGVO)*

ARBEITSTEILIGE VERARBEITUNG
EXKURS: *AUFTRAGSVERARBEITUNGSVERTRAG (AVV)*



Im Rahmen des Vertrags zu regeln

- Stand und Dauer der Verarbeitung Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Personen
- Rechte und Pflichten des Verantwortlichen
- Verarbeitung darf nur entsprechend dokumentierter Weisung des Verantwortlichen erfolgen
- Verpflichtung auf Vertraulichkeit
- Einhaltung der TOM
- Bedingungen für die Inanspruchnahme weiterer Auftragsverarbeiter
- Unterstützung des Verantwortlichen bei der Einhaltung von Betroffenenrechten
- Unterstützung des Verantwortlichen bei seinen Verpflichtungen
- Rückgabe beziehungsweise Löschung der Daten nach Ende der Leistungserbringung
- Bereitstellung von Nachweisen der Pflichteinhaltung und Zulassen von Inspektion

Quelle: EU-DSGVO Artikel 28

DSGVO – ART DES RECHTSAKTS

Die DSGVO ist eine europäische Verordnung

Für die Ausübung der Zuständigkeiten der Union nehmen die Organe Verordnungen, Richtlinien, Beschlüsse, Empfehlungen und Stellungnahmen an.
Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.
Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.
Beschlüsse sind in allen ihren Teilen verbindlich. Sind sie an bestimmte Adressaten gerichtet, so sind sie nur für diese verbindlich.
Die Empfehlungen und Stellungnahmen sind nicht verbindlich. (Art. 288 AEUV)

Über siebzig sogenannte **Öffnungsklauseln** eröffnen die Möglichkeit der nationalen Ausgestaltung über Bundes- und Landesgesetze.

Prominente Gesetzte umfassen:

- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Landesdatenschutzgesetze
- Gesetz über den Kirchlichen Datenschutz (KDG)
- Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)
- Patientendatenschutzgesetz (PDSG)

DSGVO – SCHUTZZIEL

*Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.*

*Diese Verordnung **schützt die Grundrechte und Grundfreiheiten natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.*

*Der **freie Verkehr personenbezogener Daten in der Union** darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.*

Quelle: EU-DSGVO Artikel 1

DSGVO – ABWÄGUNG MIT ANDEREN RECHTEN

Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen.

Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und ***unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen*** *werden.*

Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

Quelle: EU-DSGVO Erwägungsgrund 4

DSGVO – GLEICHWERTIGES SCHUTZNIVEAU TROTZ NATIONALER SPIELRÄUME

*Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das **Schutzniveau** für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten **in allen Mitgliedstaaten gleichwertig** sein.*

*Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten **unionsweit gleichmäßig und einheitlich angewandt** werden.*

Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen.

*In Verbindung mit den allgemeinen und horizontalen Rechtsvorschriften über den Datenschutz zur Umsetzung der Richtlinie 95/46/EG gibt es in den Mitgliedstaaten mehrere **sektorspezifische Rechtsvorschriften** in Bereichen, die spezifischere Bestimmungen erfordern.*

*Diese Verordnung bietet den Mitgliedstaaten zudem einen **Spielraum für die Spezifizierung** ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden „**sensible Daten**“).*

Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

Quelle: EU-DSGVO Erwägungsgrund 10

DSGVO – SACHLICHER ANWENDUNGSBEREICH

Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung ***personenbezogener Daten, die in einem Dateisystem gespeichert sind*** *oder gespeichert werden sollen.*

Quelle: EU-DSGVO Artikel 2, Abs. 1

DSGVO – SACHLICHER ANWENDUNGSBEREICH

*Diese Verordnung findet **keine Anwendung** auf die Verarbeitung personenbezogener Daten:*

- *im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,*
- *durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,*
- *durch natürliche Personen zur Ausübung ausschließlich **persönlicher oder familiärer Tätigkeiten**,*
- *durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten** oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.*

Quelle: EU-DSGVO Artikel 2, Abs. 2

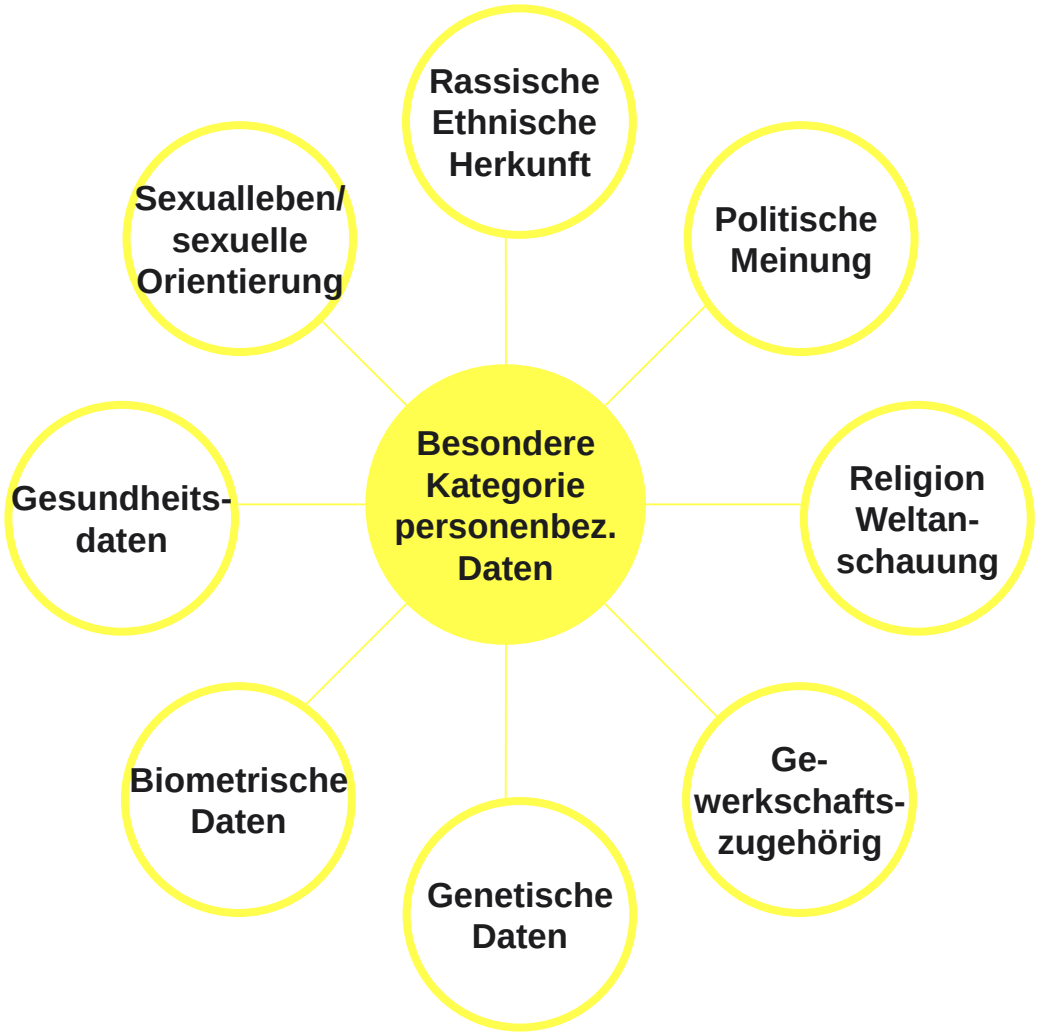
DSGVO – SACHLICHER ANWENDUNGSBEREICH

*[…] Grundsätze des Datenschutzes sollten daher **nicht für anonyme Informationen** gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.*

Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

Quelle: EU-DSGVO Erwägungsgrund 26

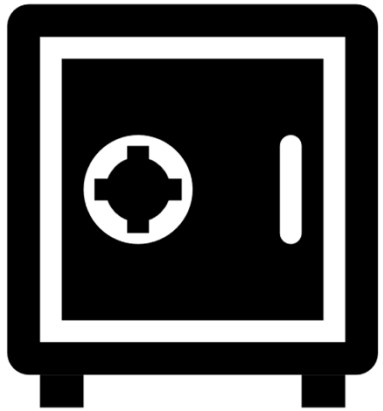
DSGVO – SACHLICHER ANWENDUNGSBEREICH BESONDERER SCHUTZ



Besondere Kategorien *personenbezogener Daten sind Datenkategorien, die durch das Gesetz einen* ***besonderen Schutz*** *erfahren (sowohl juristisch als auch technisch-organisatorisch)*

Quelle: EU-DSGVO Art. 9 Abs. 1

DSGVO – SACHLICHER ANWENDUNGSBEREICH BESONDERER SCHUTZ



*Weiterhin sind **Daten über strafrechtliche Verurteilungen und Straftaten**, sowie damit zusammenhängende Sicherungsmaßregeln **besonders geschützt**.*

→ Deren Verarbeitung darf nur unter behördlicher Aufsicht erfolgen oder wenn dies nach Unionsrecht oder dem Recht der Mitgliedsstaaten zulässig ist.

Quelle: EU-DSGVO Art. 10

DSGVO – RÄUMLICHER ANWENDUNGSBEREICH

Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese ***im Rahmen der Tätigkeiten*** *einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters* ***in der Union*** *erfolgt,* ***unabhängig davon, ob die Verarbeitung in der Union stattfindet.***

Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, ***wenn die Datenverarbeitung im Zusammenhang damit steht***

- ***betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten****, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;*
- ***das Verhalten betroffener Personen zu beobachten****, soweit ihr Verhalten in der Union erfolgt.*

Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem ***Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt****.*

Quelle: EU-DSGVO Art. 3

DSGVO – ANGRENZENDE RECHTSREGIME
EU-GRUNDRECHTECHARTA

Art. 1: Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.

Art. 8:

*(1) Jede Person hat das Recht auf **Schutz der sie betreffenden personenbezogenen Daten**.*

*(2) Diese Daten dürfen **nur nach Treu und Glauben für festgelegte Zwecke** und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das **Recht, Auskunft** über die sie betreffenden erhobenen Daten zu erhalten **und die Berichtigung** der Daten zu erwirken.*

*(3) Die Einhaltung dieser Vorschriften wird von einer **unabhängigen Stelle** überwacht.*

Quelle: EU-Grundrechtecharta Art. 1 und 8

DSGVO – ANGRENZENDE RECHTSREGIME GRUNDGESETZ

Artikel 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2:

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Quelle: Grundgesetz der BRD Art. 1

DSGVO – ANGRENZENDE RECHTSREGIME
RICHTLINIE 680 / 2016

RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die

zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von

Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

Quelle: Richtlinie 680 / 2016

DSGVO – ANGRENZENDE RECHTSREGIME KASKADE

• Europäische Ebene	**DSGVO**	Andere Verordnungen (e.g. ePrivacy)
• Nationale Ebene	**SGB I / SGB X**	Datenschutzregelungen in Spezialgesetzen (e.g. TMG)
	BDSG	Landesdatenschutzgesetz
• Sonderregelungen mit Gesetzescharakter	Tarifvertrag	Betriebsvereinbarung/ Dienstvereinbarung

DSGVO – ANGRENZENDE RECHTSREGIME
BDSG

Teil 1

- **Gemeinsame Regelungen** für öffentliche und nicht-öffentliche Stellen,
  insb. Rechtsgrundlagen für öffentliche Stellen und Videoüberwachung und zum Bundesbeauftragten für Datenschutz und die Informationsfreiheit.

Teil 2

- **Durchführungsbestimmungen zur DSGVO**, insb. Rechtsgrundlagen der Verarbeitung pbD, Rechte der betroffenen Person, Pflichten der Verantwortlichen und Auftragsverarbeiter, Aufsichtsbehörden sowie Sanktionen und Rechtsbehelfe

Teil 3

- **Datenschutz für Polizei und Justiz**
  insb. Anwendungsbereich, Rechtsgrundlagen, Betroffenenrechte, Pflichten der Verantwortlichen und Auftragsverarbeiter, Datenübermittlung an Drittstaaten, Zusammenarbeit mit den Aufsichtsbehörden, Haftung und Sanktionen

Teil 4

- **Besondere Bestimmungen** für Tätigkeiten **außerhalb der Anwendungsbereiche** der DSGVO und der JI-Richtlinie

Quelle: Bundesdatenschutzgesetz

DSGVO – AUFBAU

- **Einleitung**

  […] in Erwägung nachstehender Gründe […]

- **Erwägungsgründe**

  173 Erwägungsgründe, die darstellen, welche Zielstellungen mit den verschiedenen Rechtsnormen verfolgt werden sollen.

- **Überleitung**

  […] haben folgende Verordnung erlassen […]

- **Rechtsnormen**

  99 Artikel in 11 Kapiteln

- **Kapitel I**

  Allg. Bestimmungen

- **Kapitel II**

  Grundsätze und Rechtmäßigkeit

- **Kapitel III**

  Rechte der betroffenen Pers.

- **Kapitel IV**

  Verantwortlicher & Auftragsverarbeiter

- **Kapitel V**

  Übermittlung Drittländer

- **Kapitel VI / VII**

  Aufsicht

- **Kapitel VIII**

  Rechtsbehelfe & Sanktionen

- **Kapitel IX**

  Bes. Verarbeitungs-situationen

- **Kapitel X**

  Deligierte und Durchführungs-rechtsakte

- **Kapitel XI**

  Schluss-bestimmungen

Quelle: DSGVO

DSGVO – RECHTMÄßIGKEIT DER VERARBEITUNG

Die **Verarbeitung ist nur rechtmäßig**, wenn **mindestens eine der nachstehenden Bedingungen erfüllt ist**:

- Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen oder eines Dritten** erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. **[…]**

Quelle: DSGVO Art. 9

DSGVO – RECHTMÄßIGKEIT DER VERARBEITUNG

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, […] ist untersagt.

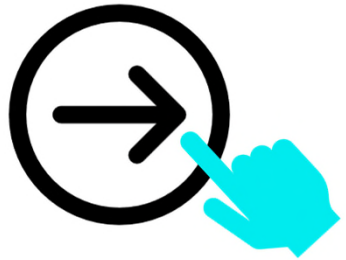
Absatz 1 gilt nicht in folgenden Fällen:

- Die betroffene Person hat […] festgelegte Zwecke ausdrücklich **eingewilligt**
- die Verarbeitung ist erforderlich, damit […] Arbeitsrecht und dem Recht der sozialen Sicherheit und des **Sozialschutzes** erwachsenden Rechte ausüben
- die Verarbeitung ist zum Schutz **lebenswichtiger Interessen** der betroffenen Person […],
- die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine […] Stiftung, Vereinigung oder sonstige **Organisation ohne Gewinnerzielungsabsicht** […]
- die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person **offensichtlich öffentlich** gemacht hat,
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei **Handlungen der Gerichte** […] erforderlich,
- die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats […] eines **erheblichen öffentlichen Interesses** erforderlich,
- die Verarbeitung ist für Zwecke der **Gesundheitsvorsorge oder der Arbeitsmedizin**, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten […]
- die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der **öffentlichen Gesundheit** […]
- die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, […] spezifische Maßnahmen zur **Wahrung der Grundrechte**

Quelle: DSGVO Art. 9

DSGVO

Übungen

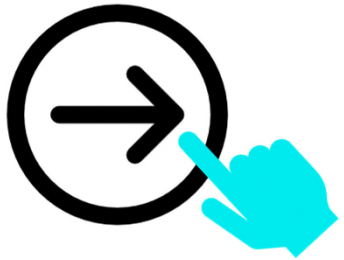


(Password: DaSchu_ITS_24)

1. Sie betreiben einen Webshop für seltene Kaugummi-Sorten. Bei der Bestellung erheben Sie Vorname, Nachname, Geburtsdatum, Adresse, Telefonnummer und Kontodaten. Ist die zur Vertragsabwicklung zu gerechtfertigten (i. S. von Art. 5 Abs. 1 DSGVO)?
2. Sie versenden als Mitarbeiter*in des obenstehenden Webshops eine E-Mail bzgl. aktueller Restposten und Sonderangebote an sämtliche Geschäfts- und Privatkunden. Die Empfängeradresse hat größtenteils die Form: vorname.nachname@unternehmen.de. Sie führen alle Adressen in CC auf. Ist der Versand (i.S. Art 5 Abs. 1) rechtmäßig?
3. Ein Kunde wendet sich an Ihr Unternehmen bzw. den DSB, da er in den Medien gehört hat, dass Sie Daten aus Social Media und von Werbepartnern aggregieren, um zugeschnittene Werbung zu versenden. Der Kunde möchte darüber informiert werden, welche Informationen von ihm im Unternehmen genutzt und verarbeitet werden. Wie sollte Ihr Unternehmen (i. S. Art 15 DSGVO) reagieren?

DSGVO

Übungen



(Password: DaSchu_ITS_24)

5. Was ist mit Unionsbezug der Datenverarbeitung gemeint?
6. Nennen Sie fünf Inhalte von Öffnungsklauseln der DSGVO.
7. Nennen Sie drei Bedingungen, die eine Rechtmäßigkeit der Verarbeitung legitimieren.
8. Nennen Sie drei Beispiele für besondere Kategorien personenbezogener Daten und Situationen in denen diese (legal) verarbeitet werden.
9. Was ist der Unterschied zwischen Pseudonymisierung und Anonymisierung? Erläutern Sie Ihre Antwort an einem Beispiel.
10. Erläutern Sie „lex specialis derogat legi generali“ anhand eines Beispiels im Bereich des Datenschutzes

FOKUS PRAXIS

Aufsichtsbehörden	**01**	**Bis 10:30 Uhr**
Der Datenschutzbeauftragte	**02**	Ca. 20 Minuten
Pflichten des Verantwortlichen	**03**	**Bis 12:15 Uhr**
Auftragsverarbeiter	**04**	Ca. 30 Minuten
Konsequenzen aus Verstößen	**05**	Ca. 5 Minuten
Risikobegriff im Datenschutz und Datenschutzfolgeabschätzung	**06**	**Bis 14:30 Uhr**

DSGVO – AUFSICHTSBEHÖRDE ZUSTÄNDIGKEIT (NATIONAL)

Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, **im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig**.

Erfolgt die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe c oder e, so ist die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig. In diesem Fall findet Artikel 56 keine Anwendung.

Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Quelle: DSGVO Art. 55

DSGVO – AUFSICHTSBEHÖRDE ZUSTÄNDIGKEIT (NATIONAL)

Bundesdatenschutzbeauftragter	Zuständigkeit	Landesdatenschutzbeauftragte(r)
• Bundesbehörden • Öffentliche Stellen des Bundes • Verarbeitungen, die zu den Erbringungen von Telekommunikationsdiensten oder Postdienstleistungen durchgeführt werden • Bundesgerichte im Rahmen der Verwaltungstätigkeiten		• nichtöffentlichen Stellen • Landesbehörden • Öffentliche Stellen des Landes • Konkrete Festlegungen im jeweiligen Landesdatenschutzrecht

DSGVO – AUFSICHTSBEHÖRDE ZUSTÄNDIGKEIT (INTERNATIONAL)

Unbeschadet des Artikels 55 ist **die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters** gemäß dem Verfahren nach Artikel 60 **die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung.**

Abweichend von Absatz 1 ist jede Aufsichtsbehörde dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen diese Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt.

In den in Absatz 2 des vorliegenden Artikels genannten Fällen unterrichtet die Aufsichtsbehörde unverzüglich die federführende Aufsichtsbehörde über diese Angelegenheit. Innerhalb einer Frist von drei Wochen nach der Unterrichtung entscheidet die federführende Aufsichtsbehörde, ob sie sich mit dem Fall gemäß dem Verfahren nach Artikel 60 befasst oder nicht, wobei sie berücksichtigt, ob der Verantwortliche oder der Auftragsverarbeiter in dem Mitgliedstaat, dessen Aufsichtsbehörde sie unterrichtet hat, eine Niederlassung hat oder nicht.

Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall zu befassen, so findet das Verfahren nach Artikel 60 Anwendung. Die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, kann dieser einen Beschlussentwurf vorlegen. Die federführende Aufsichtsbehörde trägt diesem Entwurf bei der Ausarbeitung des Beschlussentwurfs nach Artikel 60 Absatz 3 weitestgehend Rechnung.

Entscheidet die federführende Aufsichtsbehörde, sich mit dem Fall nicht selbst zu befassen, so befasst die Aufsichtsbehörde, die die federführende Aufsichtsbehörde unterrichtet hat, sich mit dem Fall gemäß den Artikeln 61 und 62.

Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung.

Quelle: DSGVO Art. 56

DSGVO – AUFSICHTSBEHÖRDE ZUSTÄNDIGKEIT - HAUPTNIEDERLASSUNG

„Hauptniederlassung“

im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die **Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen** und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; **in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung**;

im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

Quelle: DSGVO Art. 4 Abs. 16

DSGVO – AUFSICHTSBEHÖRDE AUFGABEN

Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

- die Anwendung dieser **Verordnung überwachen und durchsetzen**;
- die **Öffentlichkeit** für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung **sensibilisieren und** sie darüber **aufklären**. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;
- im Einklang mit dem Recht des Mitgliedsstaats das **nationale Parlament, die Regierung und andere Einrichtungen und Gremien** über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung **beraten**;
- die **Verantwortlichen und die Auftragsverarbeiter** für die ihnen aus dieser Verordnung entstehenden Pflichten **sensibilisieren**;
- **auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Verordnung zur Verfügung stellen** und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeiten;

Quelle: DSGVO Art. 57

DSGVO – AUFSICHTSBEHÖRDE AUFGABEN

Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

- **sich mit Beschwerden** einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 80 **befassen**, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;
- **mit anderen Aufsichtsbehörden zusammenarbeiten**, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;
- **Untersuchungen über die Anwendung dieser Verordnung durchführen**, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;
- **maßgebliche Entwicklungen verfolgen**, soweit sie sich auf den Schutz personenbezogener Daten auswirken, **insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken**;
- Standardvertragsklauseln im Sinne des Artikels 28 Absatz 8 und des Artikels 46 Absatz 2 Buchstabe d festlegen;
- eine **Liste der Verarbeitungsarten** erstellen und führen, für die gemäß Artikel 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;

Quelle: DSGVO Art. 57

DSGVO – AUFSICHTSBEHÖRDE AUFGABEN

Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

- **Beratung in Bezug auf** die in Artikel 36 Absatz 2 genannten **Verarbeitungsvorgänge** leisten;
- die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Absatz 1 fördern und zu diesen Verhaltensregeln, die ausreichende Garantien im Sinne des Artikels 40 Absatz 5 bieten müssen, **Stellungnahmen abgeben und sie billigen**;
- **die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln** und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen;
- gegebenenfalls die nach Artikel 42 Absatz 7 erteilten **Zertifizierungen regelmäßig überprüfen**;
- die **Anforderungen an die Akkreditierung einer Stelle** für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;

Quelle: DSGVO Art. 57

DSGVO – AUFSICHTSBEHÖRDE AUFGABEN

Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

- die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 vornehmen;
- Vertragsklauseln und Bestimmungen im Sinne des Artikels 46 Absatz 3 genehmigen;
- verbindliche interne Vorschriften gemäß Artikel 47 genehmigen;
- Beiträge zur Tätigkeit des Ausschusses leisten;
- interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Artikel 58 Absatz 2 ergriffene Maßnahmen und
- **jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.**

Quelle: DSGVO Art. 57

DSGVO – AUFSICHTSBEHÖRDE BEFUGNISSE

Untersuchungsbefugnisse

- Anordnung zur Herausgabe von Informationen
- Untersuchungen in Form von Datenschutzüberprüfungen
- eine Überprüfung Zertifizierungen
- Hinweise zu Verstößen geben
- Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung der DSGVO notwendig sind
- Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten

Abhilfebefugnisse

- Warnen (bei Verstößen)
- Verwarnen (bei Verstößen)
- Anweisen Betroffenenrechte umzusetzen
- Anweisen Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
- Anweisen Betroffenen zu informieren
- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
- die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung […] anzuordnen,
- eine Zertifizierung zu widerrufen
- eine Geldbuße gemäß Artikel 83 zu verhängen,
- die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

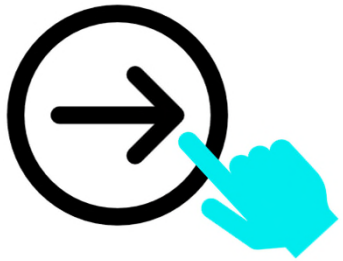
Genehmigungsbefugnisse, beratende Befugnisse

- Verantwortliche zu beraten,
- zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,
- eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln zu billigen,
- Standarddatenschutzklauseln festzulegen
- Vertragsklauseln zu genehmigen,
- Verwaltungsvereinbarungen zu genehmigen
- verbindliche interne Vorschriften genehmigen.

Quelle: DSGVO Art. 58

DSGVO

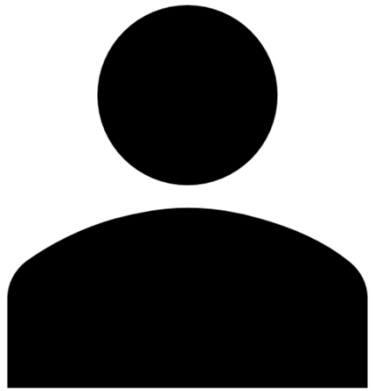
Übungen



(Password: DaSchu_ITS_24)

- Wie lautet die für Sie zuständige Aufsichtsbehörde, wenn sich die Hauptniederlassung des relevanten Verantwortlichen in Hamburg befindet.
- Recherchieren Sie die Kontaktdaten und den Namen des Landesdatenschutzbeauftragten
- Wie könne Sie einen Datenschutzbeauftragen bei der Behörde anmelden?

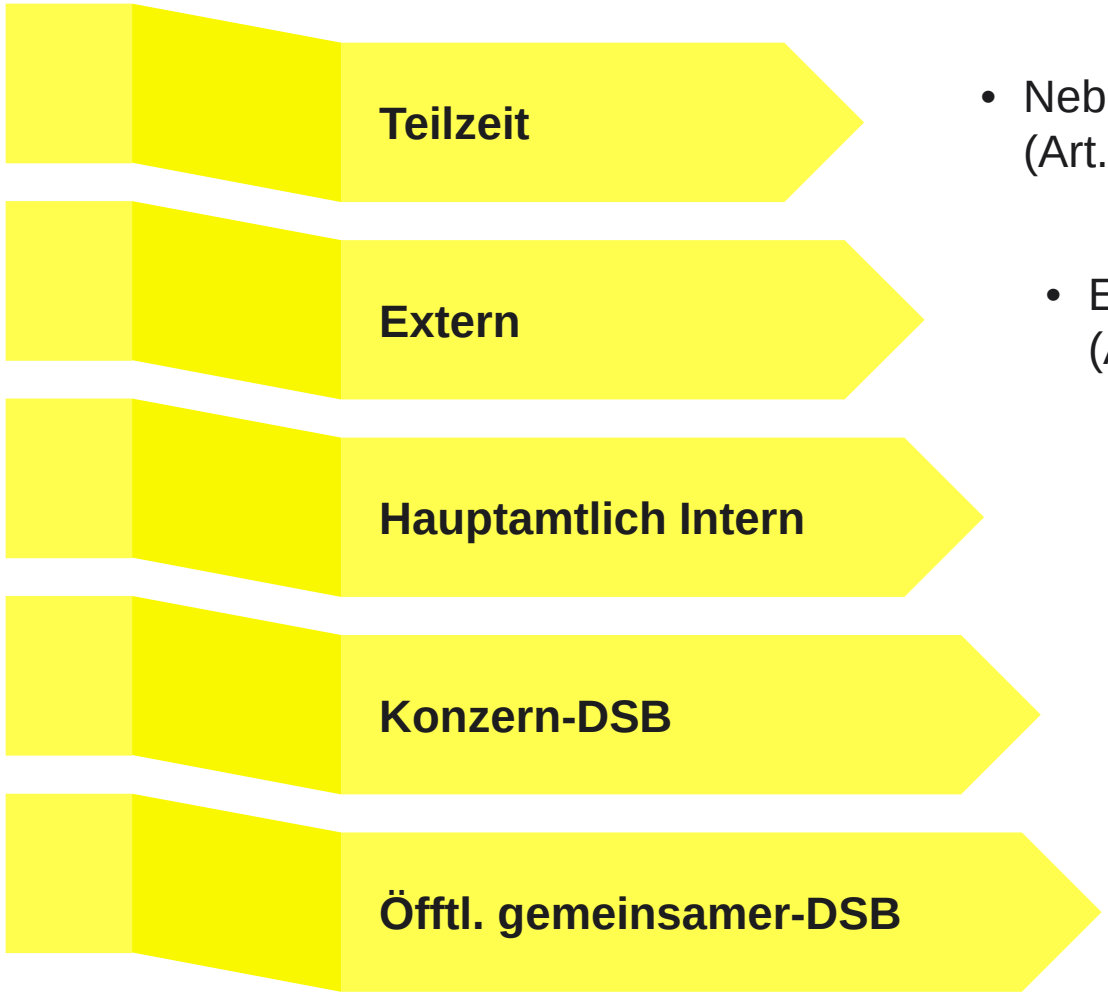
DSGVO – DER DATENSCHUTZBEAUFTRAGTE ROLLE INNERHALB DER ORGANISATION



Der Datenschutzbeauftragte…

- …fungiert als **Berater** des Verantwortlichen oder Auftragsverarbeiter im Zusammenhang mit der Verarbeitung personenbezogener Daten,
- …ist gleichzeitig das diesbezügliche **Kontrollorgan** in der Organisation und
- … ist die **Schnittstelle zu den Aufsichtsbehörden und den betroffenen Personen**, wenn diese Fragen zur Verarbeitung sie betreffender personenbezogener Daten haben.

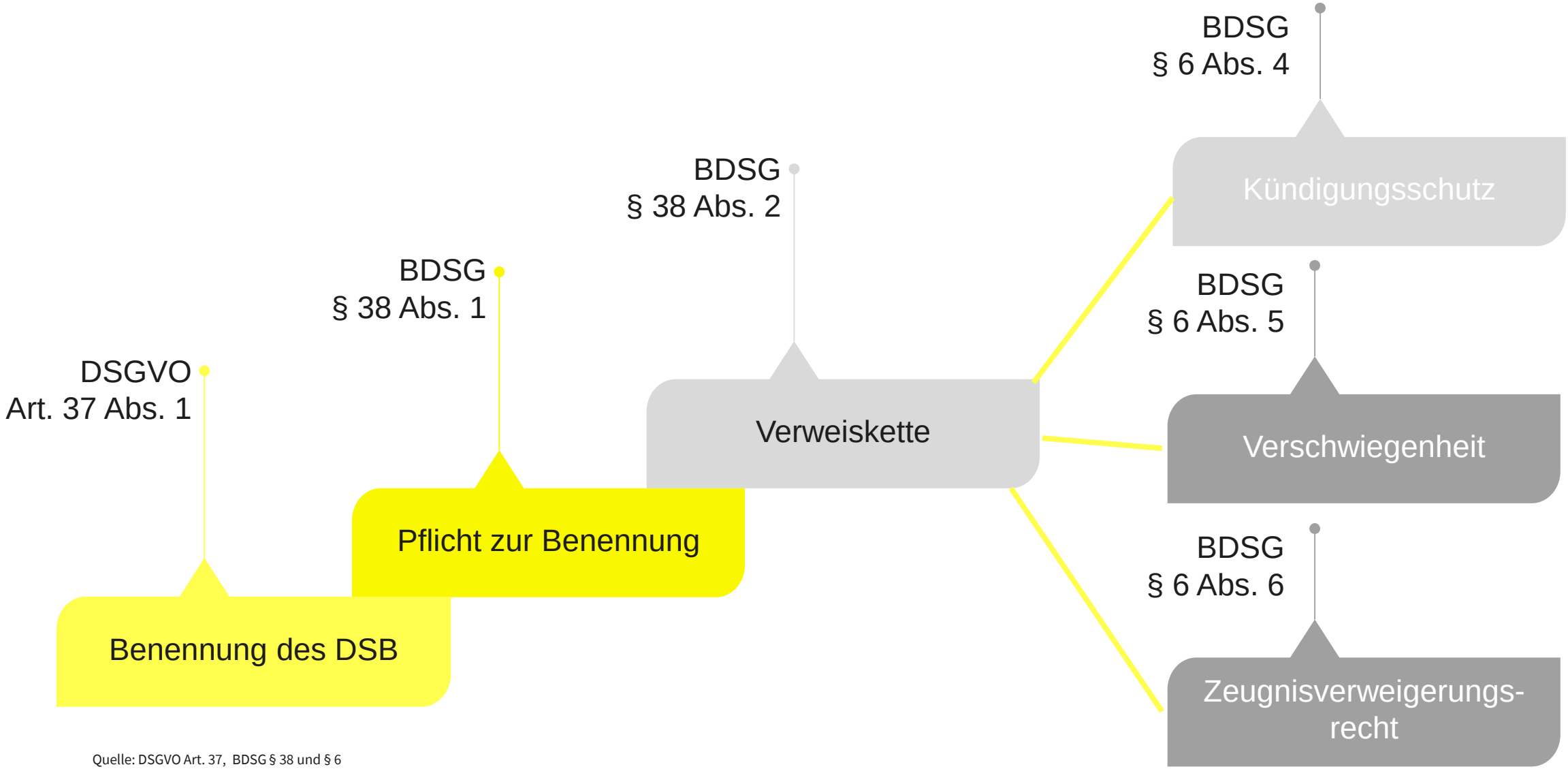
DSGVO – DER DATENSCHUTZBEAUFTRAGTE MÖGLICHKEITEN



- Nebenamtlicher interner Datenschutzbeauftragter (Art. 37 Abs. 6)
- Externer Datenschutzbeauftragter (Dienstleister) (Art. 37 Abs. 6)
- Hauptamtlicher interner Datenschutzbeauftragter (Art. 37 Abs. 6)
- Gemeinsamer Datenschutzbeauftragter innerhalb einer Unternehmensgruppe (ermöglicht Konzerndatenschutzbeauftragten – Art. 37 Abs. 2)
- Gemeinsamer Datenschutzbeauftragter für mehrere Behörden oder öffentliche Stellen (Art. 37 Abs. 3)

Quelle: DSGVO Art. 37

DSGVO – DER DATENSCHUTZBEAUFTRAGTE
BENENNUNG



Quelle: DSGVO Art. 37, BDSG § 38 und § 6

DSGVO – DER DATENSCHUTZBEAUFTRAGTE VORAUSSETZUNGEN

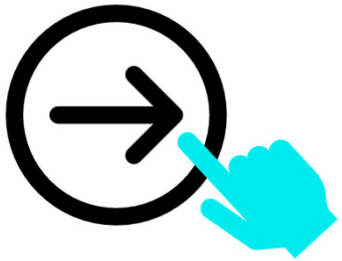
- Der Datenschutzbeauftragte wird auf der Grundlage **seiner beruflichen Qualifikation und insbesondere des Fachwissens** benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
- Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige **Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen**.

Quelle: DSGVO Art. 37 & 38

DSGVO

Übungen

10 Minuten



(Password: DaSchu_ITS_24)

- Wer ist der Datenschutzbeauftragte der IU?
- Wer ist der Datenschutzbeauftragte Ihres Partnerunternehmens?
- Nennen Sie drei Aufgaben des DSB.

DSGVO – RECHENSCHAFTSPFLICHT DES VERANTWORTLICHEN

Der Verantwortliche unterliegt einer Rechenschafts- und Nachweispflicht über…

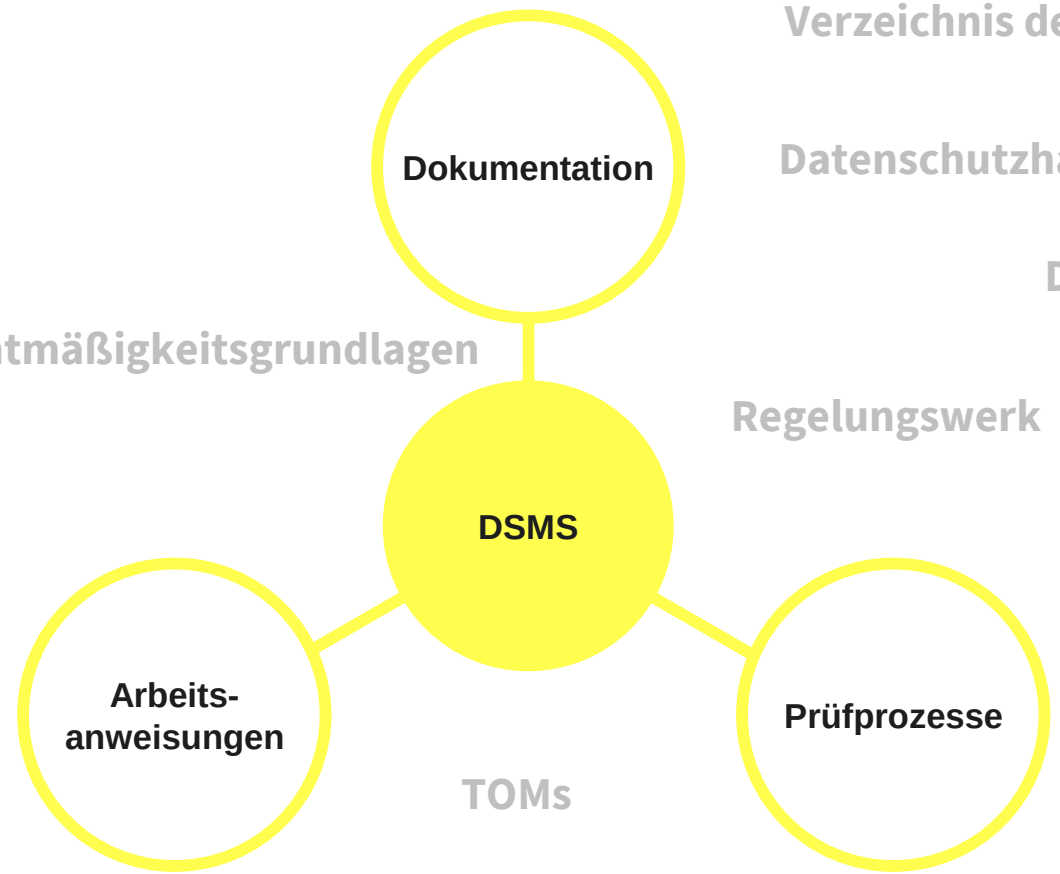
- … die **Einhaltung** (der Grundsätze) **der DSGVO** (vgl. Art. 5 Abs. 2 und Art. 24 Abs. 1)
- … die **Gewährleistung der Sicherheit** der Verarbeitung durch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der entsprechenden Maßnahmen

Der Verantwortliche muss im Rahmen der Rechenschafts- und Nachweispflicht insb.:

- Die Rechtmäßigkeit von Verarbeitungen personenbezogener Daten sicherstellen.
- Informationspflichten erfüllen
- Betroffenenrechte umsetzen
- Datenpannen melden und behandeln
- Sensibilisieren und Schulen
- Das Verzeichnis der Verarbeitungen erstellen und fortführen.

Die Einhaltung der Vorgaben impliziert eine umfangreiche Dokumentation
→ Praktische Notwendigkeit eines **Datenschutzmanagementsystems**

DSGVO – RECHENSCHAFTSPFLICHT DES VERANTWORTLICHEN - DSMS



Verzeichnis der Verarbeitungstätigkeiten

Datenschutzhandbuch

Darstellung der Zuständigkeiten

Datenschutzleitlinie

Umgang mit Dokumenten

Rechtmäßigkeitsgrundlagen

Regelungswerk

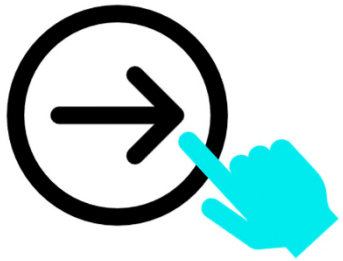
Prozessbeschreibungen

TOMs

Verpflichtungen und Schulungsnachweise

Ein Datenschutzmanagementsystem kann als die Summe aller Dokumentation und Umsetzungen von Datenschutz-bezogenen Regelungen, Prozessen und Maßnahmen definiert werden.

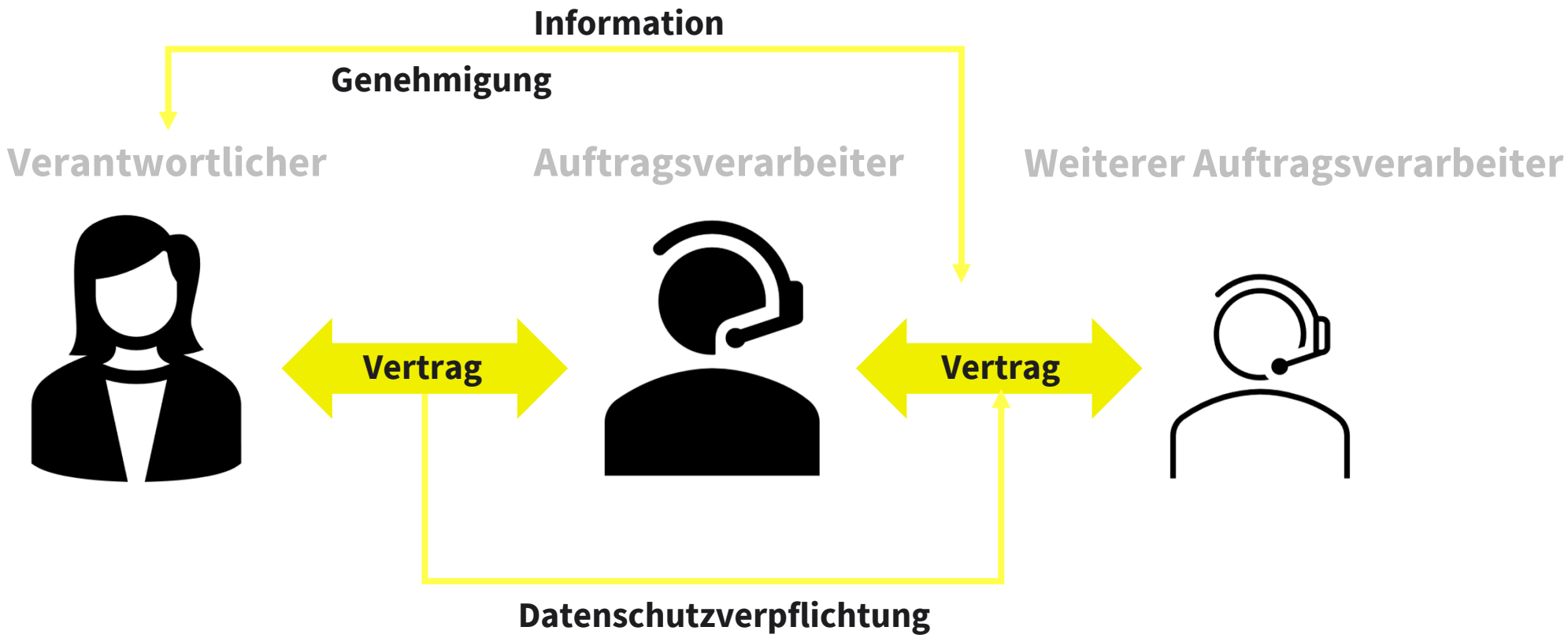
Übungen



(Password: DaSchu_ITS_24)

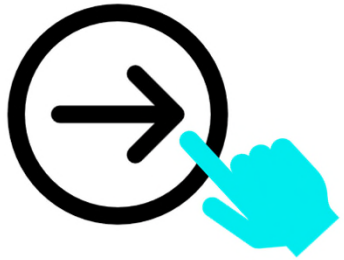
- Laden Sie die Vorlage eines VVV bei der DSK herunter: 201802_ah_muster_verantwortliche.pdf (datenschutzkonferenz-online.de)
  (→Hinweise: Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf (datenschutzzentrum.de))
- Füllen Sie die Vorlage für eine PBD-verarbeitende Tätigkeit bei Ihrem Praxispartner aus. Verändern Sie ggf. den Verarbeitungsprozesse so, dass keine Vertraulichkeitsverpflichtungen gebrochen werden.
- Diskutieren Sie in der Kleingruppe:
  - Was fällt schwer? Was ist einfach?
  - Kennen Sie den Ablageort des VVV in Ihrem Unternehmen? Waren Sie an der Erstellung oder Pflege beteiligt?
  - Wie viele Prozesse müssten schätzungsweise bei Ihrem Praxispartner erfasst werden?
- Im Anschluss: Zufällige Kleingruppe stellt das Ergebnis vor.

DSGVO – ARBEITSTEILIGE VERARBEITUNG PBD



DSGVO

Übungen



(Password: DaSchu_ITS_24)

- Stellen Sie sich vor, Sie arbeiten in einem kleinen Datenanalyse-Start-Up, das Unternehmensdaten nach Optimierungspotenzialen durchsucht. Sie greifen dabei insbesondere auf die Lohndaten und Krankheitstage je Mitarbeiter zu. Als Werkzeuge haben Sie M365 und Power BI Service im Einsatz.
- Im Rahmen einer Beauftragung treten Sie als Auftragsverarbeiter auf. Füllen Sie einen entsprechenden AVV aus: muster_adv_Version_13022018 (bayern.de) (Treffen Sie begründete Annahmen, wo notwendig)
- Suchen Sie eine Vorlage für typische „TOMs“ und diskutieren Sie, was Ihnen als Start-Up wahrscheinlich leichter und was schwerer fällt.

DSGVO – HAFTUNG UND SCHADENSERSATZ

- **Jede Person**, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, **hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter**.
- Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. **Ein Auftragsverarbeiter haftet** für den durch eine Verarbeitung verursachten Schaden **nur dann, wenn** er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser **Verordnung nicht nachgekommen** ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.
- Der Verantwortliche oder der Auftragsverarbeiter wird **von der Haftung gemäß Absatz 2 befreit, wenn er** nachweist, dass er **in keinerlei Hinsicht für den Umstand**, durch den der Schaden eingetreten ist, **verantwortlich ist**. […]
- Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, **von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern**, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

Quelle: DSGVO Art. 82 1,2,3,5

DSGVO – SCHADENSHÖHE

- Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 **Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
  - die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
  - die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
  - die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

Quelle: DSGVO Art. 83 Abs 4

DSGVO – SCHADENSHÖHE

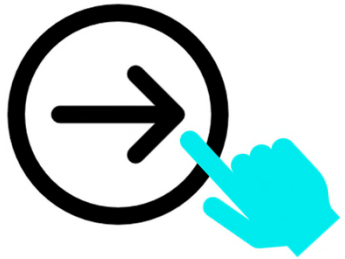
- Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 **Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
  - die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
  - die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
  - die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
  - alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
  - Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

Quelle: DSGVO Art. 83 Abs 5

DSGVO

Übungen

5 Minuten



(Password: DaSchu_ITS_24)

— Recherchieren Sie die höchsten drei Strafen gegen deutsche Unternehmen in den letzten drei Jahren.

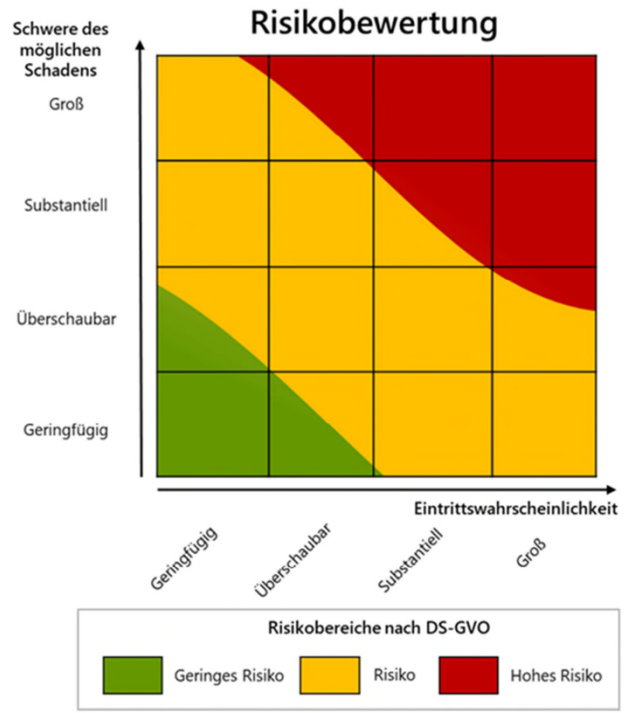
DSGVO – RISIKOBASIERTER ANSATZ

Die DSGVO zielt an diversen Stellen auf einen risikobasierten Ansatz ab. Der Begriff des Risikos wird aber nicht explizit definiert. Die Erwägungsgründe 74-76 lassen aber eine abgeleitete Definition zu.

§

E.g. Art. 32 Abs. 2:

- Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die **Risiken zu berücksichtigen**, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.



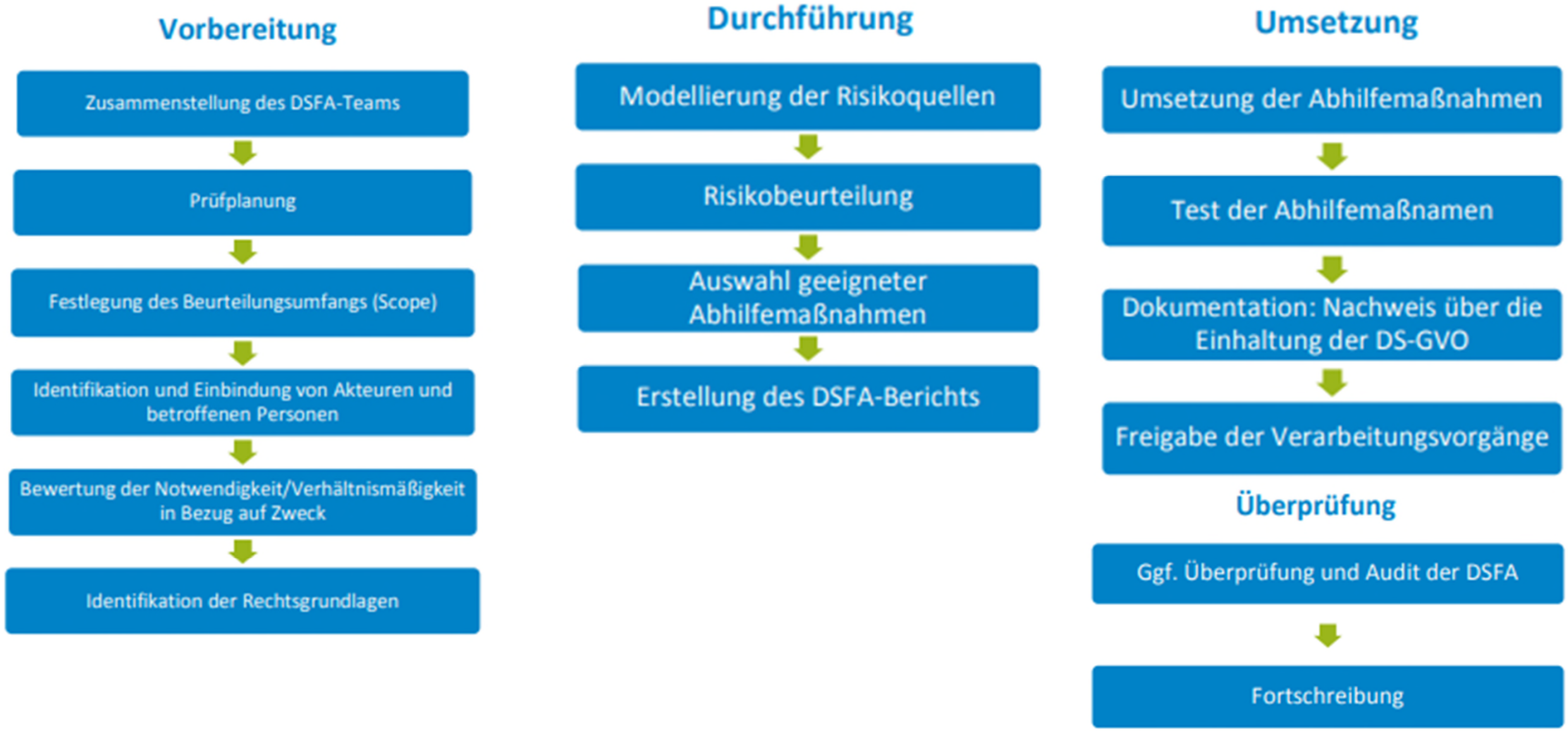
Quelle: DSGVO Art. 32 Abs. 2 und Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0).

DSGVO – DATENSCHUTZ-FOLGENABSCHÄTZUNG

- **Hat eine Form der Verarbeitung**, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.
- Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.
- Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:
  - **systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen,** die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
  - umfangreiche **Verarbeitung besonderer Kategorien von personenbezogenen Daten** gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
  - **systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**.

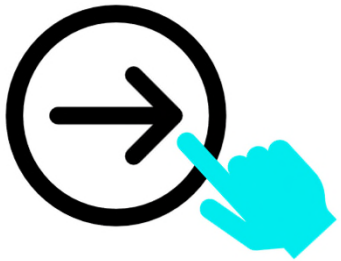
Quelle: DSGVO Art. 35 Abs. 1-3

DSGVO – DATENSCHUTZ-FOLGENABSCHÄTZUNG



Quelle: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Kurzpapier Nr. 5 – Version 2.0 (www.govdata.de/dl-de/by-2-0).

Übungen



(Password: DaSchu_ITS_24)

- Lesen Sie das Kurzpapier zur Datenschutz-Folgenabschätzung der DSK DSK_KPNr_5_Datenschutz-Folgenabschätzung_Lizenzvermerk (datenschutzkonferenz-online.de)
- Laden Sie das erläuternde Dokument zur Datenschutzfolgenabschätzung der Corona-Warn-App (CWA) herunter: 2022-10-10-CWA_DSFA-Bericht_Release_V2_25 (coronawarn.app)
- Sortieren Sie die Seitenzahlen des vorgenannten Dokuments zur CWA den einzelnen Schritten einer Datenschutzfolgeabschätzung zu.
- Wählen Sie das aus Ihrer Sicht gravierendste Risiko, welches im Dokument behandelt wird und diskutieren Sie die abgeleiteten Maßnahmen. Sind diese Maßnahmen aus Ihrer Sicht sinnvoll und ausreichend? Würden Ihnen weitere Maßnahmen einfallen?