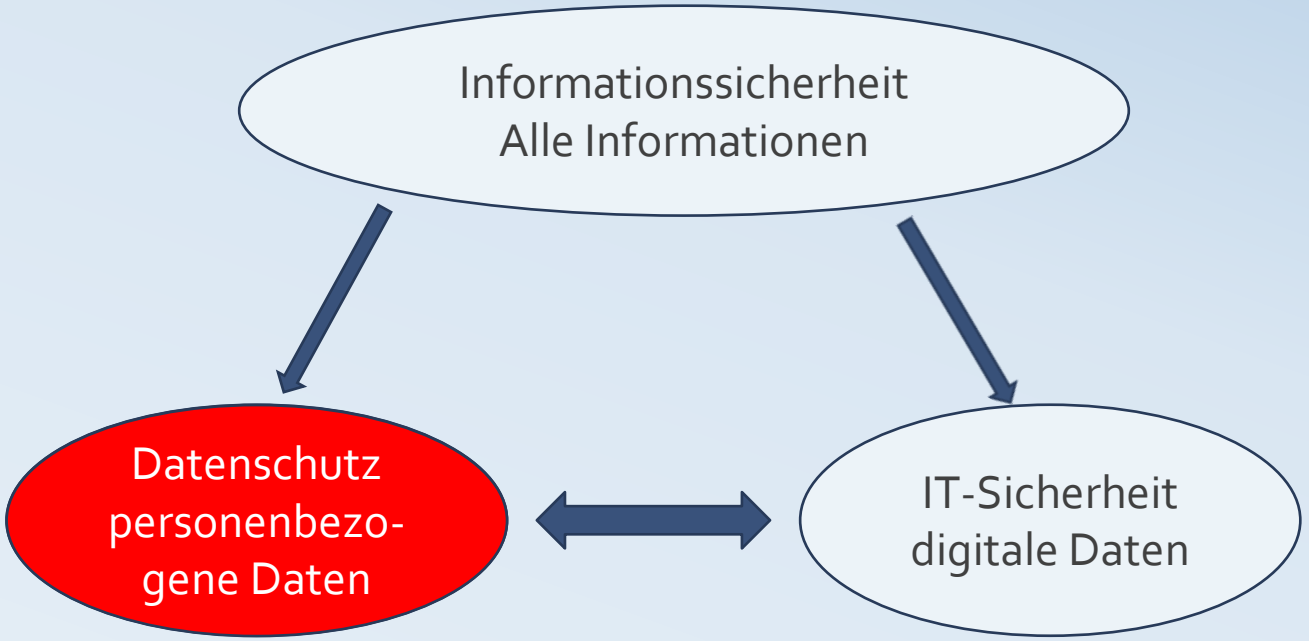
Was Fachinformatiker über Datenschutz wissen sollten

Datenschutz
Prüfungsvorbereitung IT

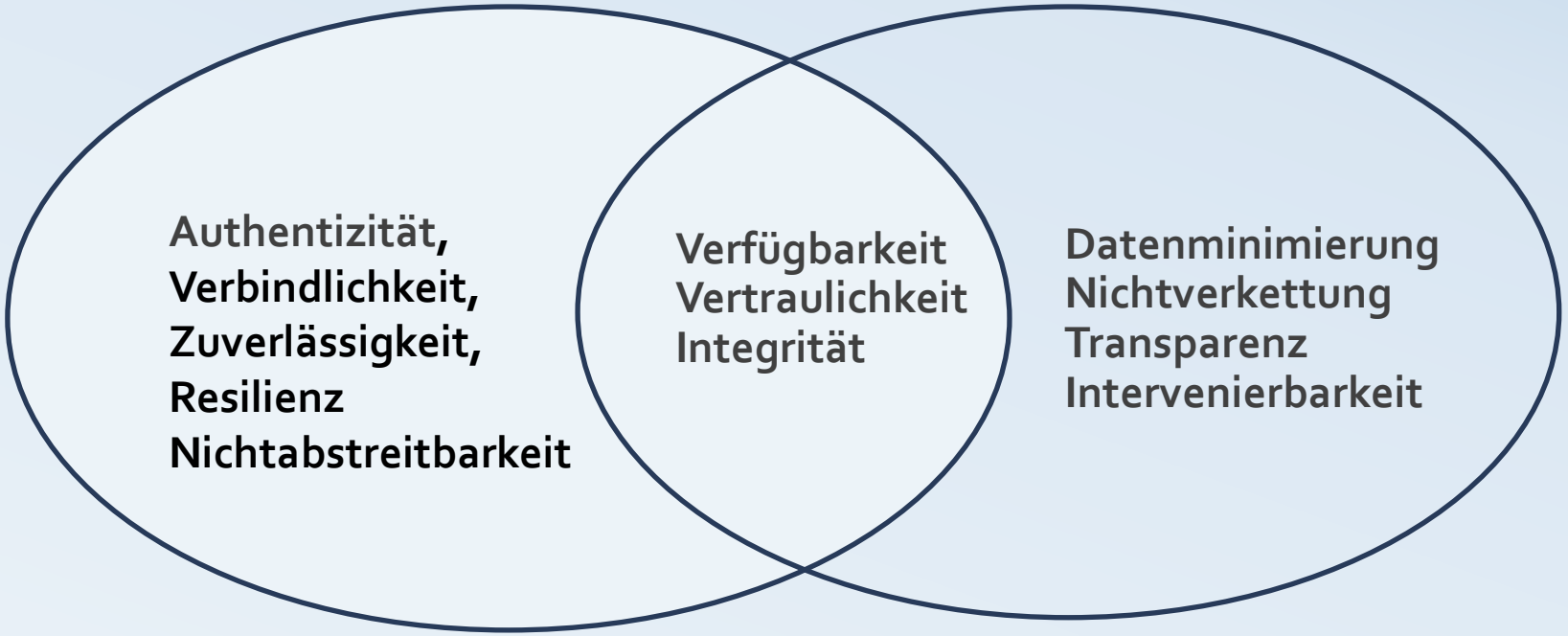
Die DSGVO im Kontext der Informationssicherheit

DSB-5seenland.de



Schutzziele/Gewährleistungsziele

Was im Verkehr die Vorfahrtsregeln, sind in der Informationssicherheit die Schutzziele, bzw. die Gewährleistungsziele



Datenschutz – rechtliche Grundlagen

EU-Grundrechte-Charta (GRCh)
Artikel 8 GRCh Schutz personenbezogener Daten

- (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.

Datenschutz – rechtliche Grundlagen

Grundgesetz der Bundesrepublik Deutschland
Artikel 2, GG

- (1) Jeder hat das Recht auf freie Entfaltung der 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 einer Person ist unverletzlich. In diese Gesetze darf nur aufgrund eines Gesetzes eingegriffen werden
- Das ist das Recht auf informationelle Selbstbestimmung

Datenschutz – rechtliche Konkretisierung

DSB-5seenland.de

Europäisches Recht

DSGVO: Umsetzung zum 25.5.2018

Deutsches Recht (ergänzend)

Bundesdatenschutzgesetz (BDSG) von 2018

Zusammengefasst: Das Recht auf „informationelle Selbstbestimmung“

DSGVO – Was sind personenbezogene Daten?

DSB-5seenland.de

Personenbezogene Daten (pbD) sind……

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen . (Art4 Abs.1)

Allgemeine pbD:
Personendaten, Kommunikations-daten, wirtschaftliche Verhältnisse, Lebens- und Konsumgewohnheiten, Qualifikationsdaten

Besondere Kategorien von pbD:
Gesundheitsdaten, biometrische/ genetische Daten, rassische/ ethnische Daten, religiöse/ ideologische Überzeugung

DSGVO Der Lebenslauf personenbezogener Daten

DSB-5seenland.de

Die „Geburt" der Daten:
Erheben, erfassen, erfragen

Das „Leben" der Daten:
Organisation, Ordnen, Speichern, die Anpassen, Verändern, Auslesen, Abfragen, Verwendung, Offenlegen, Verbreiten, Abgleichen, Verknüpfen, Einschränken

Der „Tod" der Daten:
Löschen, vernichten

DSGVO – Die beteiligten Parteien

Verantwortliche Stelle
(juristische oder natürliche Person) entscheidet über Zwecke und Mittel der Verarbeitung

Betroffene Personen
Jede natürliche Person, deren Daten verarbeitet werden

Dritte/Datenempfänger
Juristische oder natürliche Person, der pbD offengelegt werden und die unter der unmittelbaren Verantwortung des Verantwortlichen befugt ist, pbD zu verarbeiten

Auftragsverarbeiter
Stelle die pbD im Auftrag und auf Weisung des Verantwortlichen verarbeitet

DSGVO – im Unternehmenskontext

DSB-5seenland.de

Verantwortliche Stelle

- Die Verantwortung für die Einhaltung des Datenschutzes liegt immer in der Leitungsebene
- Sie muss die benötigten Ressourcen bereitstellen
- Sie hat für die Einrichtung einer Datenschutzorganisation zu sorgen
- Sie benennt ggf. den Datenschutz-beauftragten oder –koordinator
- Sie ist verantwortlich für die Meldung von Verstößen an die Aufsichtsbehörde
- Einzelne Zuständigkeiten können delegiert werden.

Abteilungen/Mitarbeitende

- Zuständig für die Erfüllung von Transparenz- und Informationspflichten
- Gestaltung von Prozessen und den entsprechenden Richtlinien und Arbeitsanweisungen
- Beachtung der Datenschutz-vorschriften bei der Gestaltung von Prozessen und Technik
- Überwachung der Einhaltung der Richtlinien und Arbeitsanweisungen
- Umsetzung der Betroffenenrechte
- Meldung von Datenschutzvorfällen

Der Datenschutzbeauftragte (DSB)

- Berichtet direkt an die oberste Managementebene
- Hat einen Datenschutz-Beratungsauftrag
- Hält Kurse zur Mitarbeiter-sensibilisierung und –schulung
- Kontrolliert die Datenschutz-dokumente
- Übernimmt das Monitoring der Umsetzung der internen Datenschutz-Management Organisation
- Arbeitet Risikoorientiert

Grundsätze für die Verarbeitung personenbezogener Daten;
Art.5 DSGVO
(1)Personenbezogene Daten müssen

a) auf rechtmäßige Weise, ... in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden

Das Recht auf „informationelle Selbstbestimmung“

- Wie kann ich das ausüben?
- Was benötige ich für eine Entscheidung?
- Was für Informationen?

Die Grundsätze der DSGVO (Art.5)

DSB-5seenland.de

Datenschutz Grundsätze

Grundsätze für die Verarbeitung personenbezogener Daten; Art.5 DSGVO

(1)Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („**Rechtmäßigkeit**, Verarbeitung nach Treu und Glauben, **Transparenz**“);

b) für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung **notwendige Maß beschränkt** sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

Datenschutz Grundsätze (2)

e) in einer Form gespeichert werden, die die **Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich** ist;.....

f) in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen **(„Integrität und Vertraulichkeit");**

(2)Der **Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich** und muss dessen Einhaltung nachweisen können **(„Rechenschaftspflicht").** Artikel

Aufgabe

Ausgangssituation:
In einer Franchise-Fitnesskette mit Filialen in ganz Europa werden die personenbezogenen Daten u.a. der Mitglieder verarbeitet. Die Firmensprache ist englisch, daher wird auch die DSGVO (GDPR) auf englisch ausgelegt. Als Mitarbeiter erhalten Sie die die Aufgabe, nachstehende Begriffe der GDPR auf deutsch zu interpretieren.

a) Personal data shall be processed in a transparent manner in relation to the data subject (lawfulness, fairness, and transparency)
b) Personal data shall be collected for specified explicit and legitimate purposes and no further in a manner that ist incompatible with the initial purposes (Purpose limitation)

Lösung:

a) Grundsatz Art.5,1 PbD müssen in rechtmäßiger Weise nach Treu und Glauben und für die betroffene Person nachvollziehbar verarbeitet werden. D.h. Nicht ohne Rechtsgrundlage und nicht ohne Datenschutzinformation.

b) Die PbD dürfen nur für vor der Verarbeitung festgelegte, legitime und eindeutige Zwecke verarbeitet werden und nicht auf eine Weise, die diesen Zwecken nicht entspricht.

Über die Rechtsgrundlagen a) und die Zwecke b) ist die Betroffene Person zu informieren

Rechtmäßigkeit

Rechtmäßigkeit
Personenbezogene Daten dürfen nur dann erhoben und verarbeitet werden, wenn es eine **Rechtsnorm** oder der **Betroffene erlaubt**.

Artikel 6
Rechtmäßigkeit der Verarbeitung
(1)Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre **Einwilligun**g zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) 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;

Rechtmäßigkeit

c) Die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

d) Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) 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;

f) 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.

Zweckbindung

Zweckbindung
Personenbezogene Daten dürfen nur zu den Zwecken verwendet werden, über die der Betroffene bei der Erhebung **informiert** wurde und denen er **zugestimmt** hat .

Artikel 5
Grundsätze für die Verarbeitung
Personenbezogene Daten müssen:
b) für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 **nicht** als unvereinbar mit den ursprünglichen Zwecken **(„Zweckbindung**“);

Videoüberwachung

DSB-5seenland.de

Aufgabe 13

Ausgangssituation: Ihr Ausbildungsbetrieb, die AMAG MED GmbH ist spezialisiert auf digitale Lösungen für die Gesundheitsbranche und managt die digitalen Prozesse eines medizinischen Pflege- und Versorgungszentrums (MPVZ). 25 Mitarbeiter des MPVZ haben Zugriff auf die Patientendaten und müssen diese elektronisch speichern und versenden. Übersendung und Speicherung von Patientendaten können aus datenschutzrechtlichen Gründen nicht im Klartext erfolgen. Es muss ebenfalls sichergestellt sein, dass kein Unbefugter Zugriff auf die Daten hat. Sie sollen das MPVZ in dieser Richtung beraten.

a) Erläutern Sie, warum Patientendaten gem. DSGVO besonders behandelt werden müssen
b) Beschreiben Sie, welche Vorgaben der DSGVO in Bezug auf die Patientendaten beachtet und umgesetzt werden müssen

Lösung:

a) Patientendaten gehören zu den besonders schützenswerten/sensiblen Daten des Art. 9 der DSGVO

b) Benennung eines DSB, Vorabkontrolle der zu übersendenden Daten (Zweckbindung, Datenminimierung)

Transparenz

Transparenz
Der Betroffene muss **eindeutig** und in **einfacher** Sprache über **Rechtsgrundlage**, **Zweckbindung** und **Informations-** und **Löschungsrechte** informiert werden.

Artikel 12

Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, **in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln**; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.
Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

Transparenz - Informationspflicht

DSB-5seenland.de

Artikel 13

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1)Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des **Verantwortlichen** sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des **Datenschutzbeauftragte**n;
c) die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** oder eine **internationale Organisation** zu übermitteln
g) die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

Transparenz – Informationspflicht (2)

DSB-5seenland.de

h) das Bestehen eines **Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf **Berichtigung** oder **Löschung** oder auf **Einschränkung der Verarbeitung** oder eines **Widerspruchsrechts** gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

i) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die **Einwilligung jederzeit zu widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

j) das Bestehen eines **Beschwerderechts bei einer Aufsichtsbehörde**;

k) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

l) das Bestehen einer **automatisierten Entscheidungsfindung einschließlich Profiling** gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Die **Datenschutzerklärung** einer Webseite muss genau beschreiben, was die Webseite im Hinblick auf die Verarbeitung personenbezogener Daten macht!

Die **Datenschutzhinweise/Transparenzerklärung** im normalen Geschäftsverkehr informieren den Kunden über seine Rechte, die Zwecke der Verarbeitung, die Speicherdauer und an wen die Daten weitergegeben werden

TTDSG

Grundsatz § 25 Abs. 1 TTDSG

Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer **eingewilligt** hat.

Ausnahme § 25 Abs. 2 TTDSG

...

1. wenn der alleinige Zweck [...] die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder

2. wenn [...] unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Aufgabe

Ausgangssituation:
Für den zielgruppengerechten Einsatz des Newsletters sollen Tracking-Cookies eingesetzt werden.
a) Erläutern Sie den technischen Begriff Cookie

b) Nennen Sie zwei Voraussetzungen, unter denen Cookies auf der Webseite rechtssicher eingesetzt werden können

Lösung:
Cookies sind kleine Dateien, die auf dem Rechner des Empfängers installiert werden und auf die Browser und Server zugreifen können. Tracking Cookies verarbeiten PbD.

- aktive Einwilligungs- Abwahlmöglichkeit des Empfängers (Cookie-Banner)

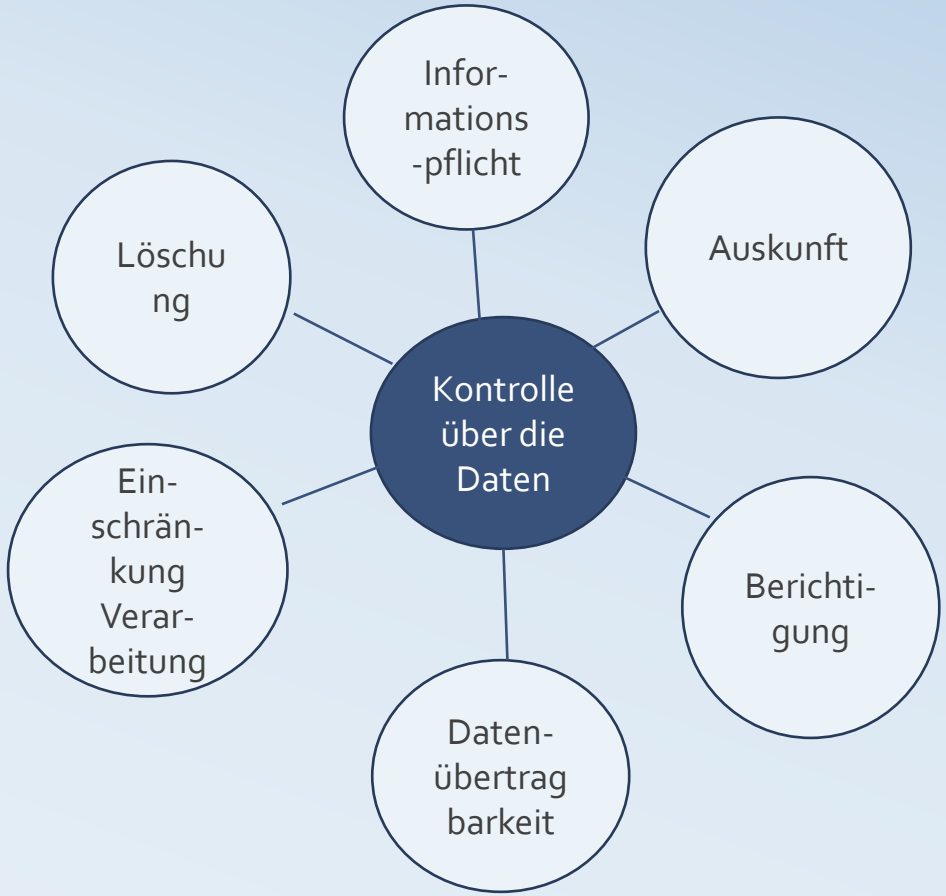
- Informationen über Art, Funktionsweise und Lebensdauer der Cookies

Transparenz - Betroffenenrechte

DSB-5seenland.de

Unter „Betroffenenrechte“ werden die Rechte der betroffenen Person gegenüber der für die Verarbeitung verantwortlichen Stelle verstanden.

Über diese Rechte ist die betroffene Person zu informieren damit sie das Selbstbestimmungsrecht ausüben kann



Aufgabe

Ausgangssituation:
Dem Nutzer einer Banking-App stehen aus dem Datenschutz bestimmte Rechte zu. Nennen Sie fünf in der DSGVO garantierte Betroffenenrechte.

Lösung:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung/Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch der Verarbeitung
- Beschwerderecht bei einer Aufsichtsbehörde

Transparenz - Informationspflicht

DSB-5seenland.de

Artikel 13

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1)Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des **Verantwortlichen** sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des **Datenschutzbeauftragte**n;
c) die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** oder eine **internationale Organisation** zu übermitteln
g) die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

Transparenz – Informationspflicht (2)

DSB-5seenland.de

h) das Bestehen eines **Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf **Berichtigung** oder **Löschung** oder auf **Einschränkung der Verarbeitung** oder eines **Widerspruchsrechts** gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

i) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die **Einwilligung jederzeit zu widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

j) das Bestehen eines **Beschwerderechts bei einer Aufsichtsbehörde**;

k) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

l) das Bestehen einer **automatisierten Entscheidungsfindung einschließlich Profiling** gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Datensparsamkeit/Datenminimierung

Datenminimierung

Es dürfen nur die Daten erhoben und gespeichert werden, die zur Erfüllung einer **speziellen Aufgabe** oder im Rahmen der **Zweckbindung** notwendig sind

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen:

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

Speicherbegrenzung

Datensicherheit und Speicherbegrenzung

Artikel 5
Grundsätze für die Verarbeitung personenbezogener Daten
Personenbezogene Daten müssen:

e) in einer Form gespeichert werden, die **die Identifizierung der betroffenen Personen** nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; („Speicherbegrenzung")…….

Löschkonzept

DSB5seenland

Wann müssen personenbezogene Daten gelöscht werden:

- Wenn sie für den Zweck der Erhebung nicht mehr benötigt werden
- Wenn die betroffene Person es verlangt (Recht auf Vergessenwerden)
- Wenn die Aufbewahrungsfristen auf Basis einer Rechtsvorschrift abgelaufen sind

…und alle Löschungen müssen dokumentiert werden (Art.5, 2 DSGVO Rechenschaftspflicht/Löschkonzept)

Löschkonzept

DSB5seenland

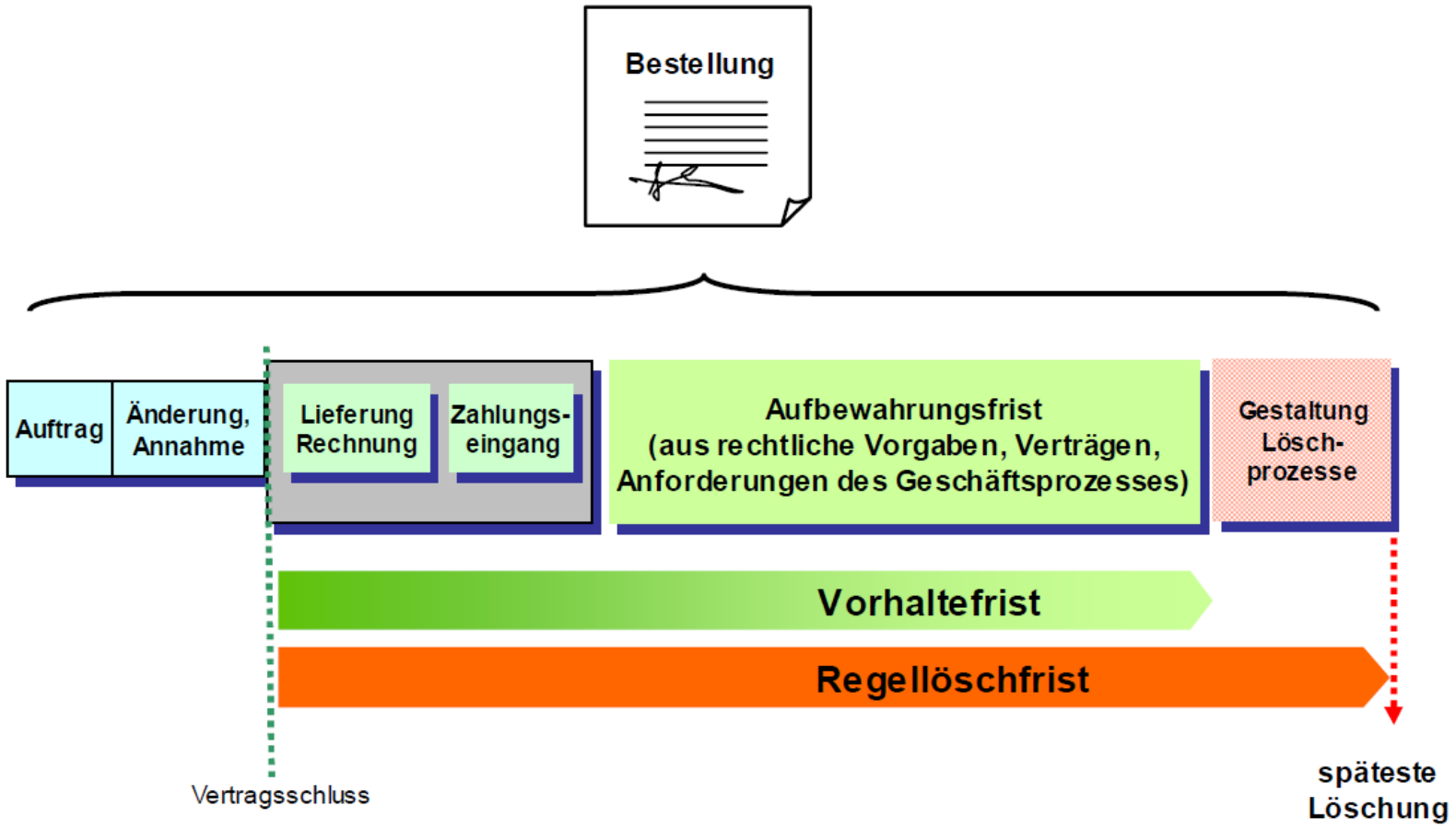
Zuständige Norm: DIN 66398

Der Leitfaden zur DIN 66398 strukturiert das Löschkonzept in 6 einzelne Schritte

DSB5seenland

Schritt 2 – Löschregeln

Abbildung 1: Beispiel für Fristabschnitte für einen Auftrag im Löschkonzept



Im Beispiel beginnt der Lauf der Vorhalte- und der Regellöschfrist mit dem Vertragsschluss. Der Vertragsschluss ist ein Beispiel für einen Startzeitpunkt vom Typ „Ende eines Vorgangs“. Die aktive Verwendung des Vertrages endet mit dem Zahlungseingang. Danach wird der Vertrag noch für eventuelle Garantiefälle und als Handelsbrief nach AO und HGB aufbewahrt.

Aufgabe 6

Ausgangssituation:
Im Zuge der Migration aus der Zentrale eines Bäckereibetriebes erhalten Sie eine Festplatte mit:

1. Eingescannten Originalen einer Umfrage zur Kundenzufriedenheit, die fertig ausgewertet ist und gelöscht werden kann. Sie enthält Name , Adresse, Geburtsdatum und Lieblingsfiliale, etc.
2. Rechnungen über Lieferungen an eine Hotelkette aus den letzte drei Jahren

Begründen Sie, welche der Daten gelöscht werden können und warum aus datenschutzrechtlicher Sicht das Formatieren und Löschen nicht ausreicht

Lösung:

Die Umfrage ist ausgewertet und der Zweck damit erfüllt. Eine gesetzliche Aufbewahrungsfrist dafür gibt es nicht. Die Daten können also gelöscht werden

Rechnungen haben 10 Jahre Aufbewahrungsfrist und Lieferscheine 6 Jahre. Die können also nicht gelöscht werden. Sie müssen aber dem allgemeinen Zugriff entzogen werden (Pseudonymisierung, Einschränkung Zugriffsrechte)

Nach den Formatierungs-, Löschvorgängen können die Daten mit entsprechenden Mitteln wiederhergestellt werden.

Integrität und Vertraulichkeit

Datensicherheit und Speicherbegrenzung

Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen:

f) in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete **technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit");

Datensicherheit und Speicherbegrenzung

Kategorien der TOM:

- Zutrittskontrolle – Schutzziel Vertraulichkeit
- Zugangskontrolle – Schutzziel Vertraulichkeit
- Zugriffskontrolle – Schutzziel Vertraulichkeit
- Pseudonymisierung/Anonymisierung - Schutzziel Vertraulichkeit
- Weitergabekontrolle – Schutzziel Integrität
- Eingabekontrolle – Schutzziel Integrität
- Verfügbarkeitskontrolle – Schutzziel Verfügbarkeit
- Regelmäßige Überprüfung und Aktualisierung durch Datenschutzmanagement

Technisch-organisatorische Maßnahmen
TOM

Aufgabe

Ausgangssituation:
Bei Recherchen zur Sicherheit um das Betriebssystem hat das BSI verschiedene Empfehlungen veröffentlicht. Insbesondere „Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10".
Beschreiben Sie die besonderen Anforderungen an den Datenschutz, die bei der Protokollierung beachtet werden müssen.

Lösung:
Die Daten dürfen nur nach den Regeln der DSGVO/BDSG gespeichert und verwendet werden. Grundsatz Datenminimierung und TOM. Z.B. zentrale Speicherung und Absicherung der Logfiles, Löschkonzept

Aufgabe 9

Ausgangssituation:
Die Bau GmbH & Co wählt einen Server für Sicherungsaufgaben aus. Der Server besitzt einen RAID-Controller, der RAID 5 und RAID10 unterstützt. Gem. DSGVO müssen geeignete technisch-organisatorische Maßnahmen ergriffen werden, mit denen die Schutzziele Integrität, Verfügbarkeit und Belastbarkeit bei der Verarbeitung suchergestellt werden können.
Beschreiben Sie drei Maßnahmen, die geeignet sind, die Datensicherheit beim Dateiaustausch zu gewährleisten.

Lösung:

1. Verschlüsselung über einen VPN-Tunnel
2. Redundante Internetverbindung
3. Monitoring-Tools zur Überwachung von Server und Netzkomponenten
4. Erstellen Notfallplan

***Artikel 5, Abs.* (2)**
Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Das kann mit Hilfe des Verfahrensverzeichnisses (VVT) gem. Art. 30 DSGVO durchgeführt werden

Datensicherheit/TOM

DSB-5seenland.de

Verzeichnis von Verfahrenstätigkeiten (VVT) Artikel 30 DSGVO

(1)Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.

Verfahren/Geschäftsprozesse

Interessentendatenverwaltung
Mitarbeiterdatenverwaltung
Bewerberdatenverwaltung
Lieferanten und Dienstleisterdatenverwaltung
Lohnbuchhaltung
Finanzbuchhaltung
Zeiterfassung
Projektplanung

Reisekostenabrechnung
Abwesenheitskalender (Urlaub, Krankheit)
Mobilgeräte Abrechnungen
Fortbildung/Schulungen
Veranstaltungsplanung
Dienstwagen/Flottenkarten
IT Inventarverzeichnis

E-Mail Postfächer
Telefonanlage
Internes Netzlaufwerk
Cloudspeicher
Konferenzsoftware
VOIP-Software
Videoüberwachung
Alarmanlage
Türschlösser
Tresorschloss

E-Mail-Marketing
Kontaktformular
Google Analytics
Facebook Pixel
Remotezugriff
Fernwartung Software
Backup
Archivierung
IT-Support/ IT-Wartung
Antivirus-System
Passwortmanager
Benutzerverwaltung
Gastzugang (WLAN)

VVT - Muster

DSB-5seenland.de

VVT HOWTO

VVT Schule

VVT Industrie

VVT Kita

Auftragsverarbeitung Art. 28 DSGVO

DSB5seenland

Art. 28 Abs. 3)
Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines **Vertrags** oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und **in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.** Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter:
a) die personenbezogenen Daten nur auf **dokumentierte Weisung des Verantwortlichen** — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet.....

Auftragsverarbeitung Art. 28 DSGVO

DSB5seenland

Art. 29

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Aufgabe 5

Ausgangssituation:
Die Firma IT-Solution GmbH, deren Mitarbeiter im IT-Bereich Sie sind, verarbeitet personenbezogene Daten im Auftrag der Bauwo AG. Die Bauwo AG verlangt daher vom Auftragnehmer die Erstellung eines Auftragsverarbeitungsvertrages (AV-Vertrag).
Was ist ein AV-Vertrag und was muss er beinhalten?

Lösung:

Der AV-Vertrag regelt das Verhältnis zwischen Auftraggeber (Verantwortliche Stelle) und Auftragnehmer (Auftragsverarbeiter). Er verpflichtet den Verarbeiter die Daten nur nach Weisung der Verantwortlichen Stelle, nach den Vorgaben der DSGVO und unter Einhaltung der angemessenen TOM zu verarbeiten.

- Vertragsgegenstand
- Anwendungsbereich,
- Behandlung Betroffenenrechte
- Informationspflichten
- Dauer der AV
- Verantwortlichkeiten
- Dokumentation
- Haftung und Schadenersatz
- Art der Verarbeitung und TOM
- Pflichten von AN und AG
- Subunternehmer

Datenschutzverstoß

Artikel 4, Ziff.12
„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Art5, Abs.1, lit. F
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)

Datenschutzverstoß

Aus Art4 und 5 ergibt sich für den Tatbestand der „Verletzung", dass es unwichtig ist, ob eine aktive Verletzungshandlung, oder eine Unterlassung vorliegt.

Der Verletzungserfolg muss durch ein **Sicherheitsdefizit** der getroffenen technischen und organisatorischen Maßnahmen hervorgerufen werden, wodurch die Integrität und Vertraulichkeit der personenbezogenen Daten gem. Art. 5 Abs. 1 lit. f DSGVO nicht gewährleistet ist.
Diese mangelhafte Sicherheit beim Verantwortlichen muss zu einer Vernichtung, einem Verlust, einer Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang personenbezogener Daten geführt haben.
Es muss sich also um eine **Vertraulichkeits-, Integritäts- oder Verfügbarkeitsverletzung** handeln.

Datenschutzverstoß

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst **binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen** führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2)Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

Datenschutzverstoß

Voraussetzung für eine Meldepflicht ist also:

- Verletzung der Integrität oder Verfügbarkeit oder Vertraulichkeit durch unzureichende TOM
- Ein Zugriff auf personenbezogene Daten erfolgt ist
- Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht
- Das Sicherheitsrisiko liegt im Verantwortungsbereich der Verantwortlichen Stelle

Datenschutzverstoß

Häufige Ursachen von Datenschutzverstößen gem. Aufsichtsbehörde Sachsen-Anhalt

Risikoansatz DSGVO-Datenschutz

DSB-5seenland.de

Schutzziele (Gewährleistungsziele gem. SDM3.0):

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Datenminimierung
- Nichtverkettung (von Zwecken)
- Transparenz
- Intervenierbarkeit

Schutzobjekte:

Rechte und Freiheiten natürlicher (betroffener) Personen

Methodik:

Standard-Datenschutzmodell 3.0 (SDM3.0)

Bewertungsmethoden

Informationssicherheit:

Quantit5ativer Ansatz, die Risiken bewertbar sind:

- Mathematisch auf Basis statistischer Auswertungen
- Mathematisch/Finanziell bei eingetretenen Schäden

Datenschutz:

Qualitativer Ansatz, da z.B. Faktoren wie:

- „Missbrauchsinteresse“,
- „Entdeckungsrisiko“
- „Risiko der unberechtigten Offenlegung“

Können nicht mathematisch erfasst werden, sondern müssen in Kategorien eingestuft werden.

Risikoanalyse - Schwellwertanalyse

DSB-5seenland.de

Schwellwertanalyse

Voraussetzung für eine Risikoanalyse ist die Durchführung einer Schwellwertanalyse. In der Schwellwertanalyse wird geprüft, ob eine Verarbeitungstätigkeit ein vermutlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, also ob eine Datenschutzfolgeabschätzung (DSFA) durchgeführt werden muss.

Risiko

Um eine Risikohöhe oder einen Schutzbedarf sowie die entsprechenden TOM's festlegen zu können, muss erst die Risikoschwere bewertet werden.

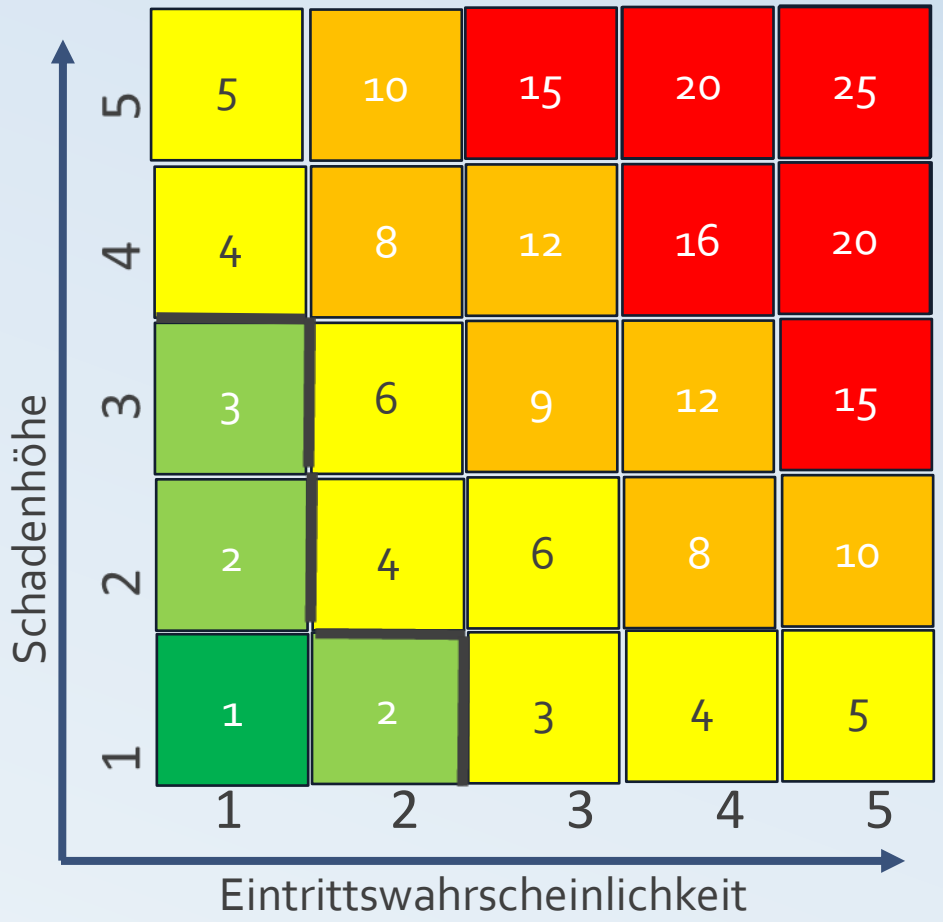
Ausmaß	X	Eintrittswahr-scheinlichkeit	=	Risikoschwere

<u>Bewertung der Risikoschwere qualitativ (Beispiel):</u>

Unwesentlich (Stufe A)	1
Gering (Stufe B)	2
Mittel (Stufe C)	3
Beherrschbar (Stufe D)	4
Kritisch (Stufe E)	5

Risikoanalyse - Risikomatrix

DSB-5seenland.de



Schutzbedarfsstufen

Unwesentlich	1
Gering	2-3
Mittel	4-6
Hoch	7-12
Kritisch	>12

Akzeptables Risiko:
Alle Risiken deren Risikoschwere >4 ist

Alle anderen müssen mit entsprechenden Maßnahmen gesichert werden

Risikoanalyse - Bewertung

DSB-5seenland.de

Verarbeitung	Risiko	Eintrittswahrs.	Schwere	Auswirkung
Personalverwaltung	ID-Diebstahl	3	5	15
	Diskriminierung	4	2	8
	Finanzielle Schäden	2	4	8
	Rufschädigung	5	3	15
	Körperlicher Schaden	1	4	4
Kundendaten	Rufschädigung	5	4	20
	Wirtschaftliche Nacht.	4	5	20
	Finanzielle Nachteile	4	4	16
	Erschwerung Rechtsausübung	1	4	4
	Kontrollverlust	5	2	10
	Profiling	2	1	2

Unwesentlich	1
Gering	2
Mittel	3
Beherrschbar	4
Kritisch	5

Schutzbedarfsstufen

Unwesentlich	1
Gering	2-3
Mittel	4-6
Hoch	7-12
Kritisch	>12

Die Einstufung richtet sich immer nach dem höchsten Einzelrisiko

Risikoanalyse - Risikobehandlung

DSB-5seenland.de

Zur Minimierung der Datenschutzrisiken werden dem Stand der Technik entsprechende TOM's eingesetzt.

Diese müssen der Art und Schwere des Risikos angemessen sein und ergeben sich aus der Schutzbedarfsanalyse. Zur Auswahl stehen bspw.:

Kategorien der TOM:

- Zutrittskontrolle – Schutzziel Vertraulichkeit
- Zugangskontrolle – Schutzziel Vertraulichkeit
- Zugriffskontrolle – Schutzziel Vertraulichkeit
- Pseudonymisierung/Anonymisierung - Schutzziel Vertraulichkeit
- Weitergabekontrolle – Schutzziel Integrität
- Eingabekontrolle – Schutzziel Integrität
- Verfügbarkeitskontrolle – Schutzziel Verfügbarkeit
- Regelmäßige Überprüfung und Aktualisierung durch Datenschutzmanagement

DSB-5seenland.de

Urheberrecht und Datenschutz

Urheberschutz – wo geregelt?

DSB-5seenland.de

Grundlagen des Urheberrechts in Deutschland sind:

- Urheberrechtsgesetz (UrhG)
- Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) seit 1.8.2021

Urheberschutz – Wie entsteht er

§ 7 Urheber
Urheber ist der Schöpfer des Werkes.

§ 8 Miturheber
(1) **Haben mehrere ein Werk gemeinsam geschaffen,** ohne dass sich ihre Anteile gesondert verwerten lassen, so sind sie Miturheber des Werkes.
(2) Das Recht zur Veröffentlichung und zur **Verwertung des Werkes steht den Miturhebern zur gesamten Hand zu**; Änderungen des Werkes sind nur mit Einwilligung der Miturheber zulässig. Ein Miturheber darf jedoch seine Einwilligung zur Veröffentlichung, Verwertung oder Änderung nicht wider Treu und Glauben verweigern. Jeder Miturheber ist berechtigt, Ansprüche aus Verletzungen des gemeinsamen Urheberrechts geltend zu machen; er kann jedoch nur Leistung an alle Miturheber verlangen

Urheberschutz – Wie entsteht er

UrhG § 10 Vermutung der Urheber- oder Rechtsinhaberschaft

(1) Wer auf den Vervielfältigungsstücken eines erschienenen Werkes oder auf dem Original eines Werkes der bildenden Künste in der üblichen Weise als Urheber bezeichnet ist, wird bis zum Beweis des Gegenteils als Urheber des Werkes angesehen; dies gilt auch für eine Bezeichnung, die als Deckname oder Künstlerzeichen des Urhebers bekannt ist.

(2) Ist der Urheber nicht nach Absatz 1 bezeichnet, so wird vermutet, dass derjenige ermächtigt ist, die Rechte des Urhebers geltend zu machen, der auf den Vervielfältigungsstücken des Werkes als Herausgeber bezeichnet ist. Ist kein Herausgeber angegeben, so wird vermutet, dass der Verleger (/Inhaber der Webseite) ermächtigt ist.

Urheberschutz – Wie entsteht er

Es empfiehlt sich also:
Das Anbringen eines Urhebervermerks: z.B. an Texten, Programmcodes und Bildern den Namen. Das erleichtert vor Gericht die Beweisführung, dass man wirklich der Urheber ist.

Das könnte z.B. Durch einen Copyright-Vermerk geschehen

Urheberschutz – was wird geschützt

DSB-5seenland.de

- Reine Ideen oder Konzepte werden im Urheberrecht nicht geschützt. Für diese gilt das Marken-/Patentrecht
- Der Schutz erstreckt sich nur auf die Nutzung der umgesetzten Ideen – die Werke.
- Die schützenswerten Werke müssen eine gewisse „Schöpfungshöhe“ aufweisen, durch die sie sich von alltäglichem unterscheiden.
- Das gilt auch für das Marken-/Patentrecht. Hier spricht man von der „Erfindungshöhe“
- Das UrhDaG schützt die urheberrechtliche Verantwortlichkeit von Upload-Plattformen wie YouTube, Vimeo, Facebook, etc.
- Das Urheberrecht greift, sobald ein Urheber sein Werk vollendet hat unabhängig von dessen Veröffentlichung
- Der Urheberschutz erlischt 70 Jahre nach dem Tod des Urhebers

Urheberschutz – Auswirkung auf Anwendungsentwicklung

DSB-5seenland.de

Betroffen hiervon sind vor allem Webentwickler, Anwendungsprogrammierer, Designer und Webseitenbetreiber

Fotos: Jedes Foto wird u.a. durch das Recht am eigenen Bild geschützt. Auch Urlaubsselfies, Screenshots oder Vorschaubilder von Bildplattformen

Videos: Bilder in Videos werden unabhängig von der Schöpfungshöhe geschützt. Gesamtwerke inkl. Schnitte, Musik, etc. wird ab einer gewissen Schöpfungshöhe als neues Werk geschützt

Texte: z.B. Werbeslogans oder Produktbeschreibungen können ab einer gewissen Schöpfungshöhe geschützt werden (Copyright)

Rechtstexte: auch AGB, Datenschutzerklärungen, Vertragstexte sind in der Regel urheberrechtlich geschützt

Musik: Texte, Melodie, Arrangement sind unabhängig von der Schöpfungshöhe geschützt

Software: Lauffähige Programme sind urheberrechtlich geschützt. Webauftritte als Gesamtheit jedoch nicht. Hier gilt das UrhG nur für einzelne Bestandteile

Datenbanken: wesentliche Inhalte von Datenbanken unterliegen als Werk dem Urheberschutz

Wissenschaftlich- technische Darstellungen: Zeichnungen, Pläne, Skizzen etc. zählen zu den geschützten Werken

Urheberrecht vs. Markenrecht

DSB-5seenland.de

Im **Urheberrechtsgesetz (UrhG)** als zentrales Gesetz sind die Rechte der geistigen Schöpfer am schutzwürdigen Werk und mögliche Maßnahmen bei Urheberrechtsverletzungen festgelegt.

Nach dem Markengesetz (MarkenG) können Unternehmen Marken, geschäftliche Bezeichnungen und auch geografische Herkunftsangaben schützen lassen.

Urheber – wer ist das und welche Rechte hat er?

DSB-5seenland.de

- Urheber ist immer eine **natürliche Person**, die ein Werk erstellt hat.
- Eine juristische Person kann nicht Urheber eines Werkes sein
- Im Unterschied zum Marken-/Patentrecht muss das Werk nirgendwo angemeldet werden.
- Sobald das „Werk" vollendet ist, greift automatisch das Urheberrecht

Die Rechte des Urhebers:

- Alleinige Entscheidung über die Nutzung und Verwertung des Werkes
- Entscheidungsrecht über die Namensnennung oder Verzicht darauf
- Urheberschaft kann nicht auf andere übertragen werden. Das gilt nur für die Nutzungs- und Verwertungsrechte
- Webdesigner, Agentur, etc. haften für die Einhaltung der Urheberrechte

Urheberrecht im Beschäftigtenkontext

§69 b UrhG :

(1) Wird ein Computerprogramm von einem Arbeitnehmer in Wahrnehmung seiner Aufgaben oder nach den Anweisungen seines Arbeitgebers geschaffen, so ist ausschließlich der Arbeitgeber zur Ausübung aller vermögensrechtlichen Befugnisse an dem Computerprogramm berechtigt, sofern nichts anderes vereinbart ist.

Urheberrecht und KI

- Generative KI-Anwendungen sind in der Lage, eigenständige Werke zu schaffen. Text, Ton Bild
- Wie sind diese Werke urheberrechtlich zu bewerten?

- Nach UrhG muss der Schöpfer eine natürliche Person sein. Nach geltender Auffassung kann also eine KI nicht Urheber sein.
- Die KI-Anwendung erzeugt ihr Ergebnis oftmals durch Training mit urheberrechtlich geschützten Werken
- D.h. in diesen Fällen müssen soweit möglich die Urheber kontaktiert und mit Ihnen ein Nutzungsvertrag geschlossen werden.
- I.d.R. erfolgt das Training auf einen oder mehrere definierte Zwecke hin. Sollen die geschützten Quelldaten auch für andere KI-Trainings verwendet werden, ist das in der Nutzungsvereinbarung zu berücksichtigen.

Urheberschutz – Verletzung von Urheberrechten

DSB-5seenland.de

§ 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke
(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit **Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe** bestraft.
(2) Der Versuch ist strafbar.

§ 107 Unzulässiges Anbringen der Urheberbezeichnung
(1) Wer
1. auf dem Original eines Werkes der bildenden Künste die Urheberbezeichnung (§ 10 Abs. 1) ohne Einwilligung des Urhebers anbringt oder ein derart bezeichnetes Original verbreitet,
2. auf einem Vervielfältigungsstück, einer Bearbeitung oder Umgestaltung eines Werkes der bildenden Künste die Urheberbezeichnung (§ 10 Abs. 1) auf eine Art anbringt, die dem Vervielfältigungsstück, der Bearbeitung oder Umgestaltung den Anschein eines Originals gibt, oder ein derart bezeichnetes Vervielfältigungsstück, eine solche Bearbeitung oder Umgestaltung verbreitet, **wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe** bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.
(2) Der Versuch ist strafbar.

Urheberdiensteanbietergesetz (UrhDaG)

Pflichten des Diensteanbieters seit 31.5.2021:

Ein Diensteanbieter ist verpflichtet, bestmögliche Anstrengungen zu unternehmen, um die vertraglichen Nutzungsrechte für die öffentliche Wiedergabe urheberrechtlich geschützter Werke zu erwerben.

Zulässig ist die öffentliche Wiedergabe von urheberrechtlich geschützten Werken und Teilen von Werken durch den Nutzer eines Diensteanbieters zu folgenden Zwecken:

1. für Zitate nach § 51 des Urheberrechtsgesetzes,
2. für Karikaturen, Parodien und Pastiches nach § 51a des Urheberrechtsgesetzes und
3. für von den Nummern 1 und 2 nicht erfasste gesetzlich erlaubte Fälle der öffentlichen Wiedergabe nach Teil1 Abschnitt 6 des Urheberrechtsgesetzes.

Datenschutz und Direktmarketing

Was ist erlaubt?

Direktwerbung – UWG §7

§ 7 Unzumutbare Belästigungen

(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.

(2) Eine unzumutbare Belästigung ist stets anzunehmen

1. bei Werbung unter Verwendung eines in den Nummern 2 und 3 nicht aufgeführten, für den Fernabsatz geeigneten Mittels der kommerziellen Kommunikation, durch die ein Verbraucher hartnäckig angesprochen wird, obwohl er dies erkennbar nicht wünscht;

2. bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung,

3. bei Werbung unter Verwendung einer automatischen Anrufmaschine, eines Faxgerätes oder elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt, **oder**

Direktwerbung – UWG §7

4. bei Werbung mit einer Nachricht,
a) bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird **oder**

b) bei der gegen § 6 Absatz 1 des Telemediengesetzes verstoßen wird oder in der der Empfänger aufgefordert wird, eine Website aufzurufen, die gegen diese Vorschrift verstößt, **oder**

c) bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Direktwerbung – UWG §7

(3) Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post **nicht** anzunehmen, wenn

1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,

2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,

3. der Kunde der Verwendung nicht widersprochen hat **und**

4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen

Werbung/Direktwerbung Rechtsgrundlagen

DSB-5seenland.de

1. Einwilligung der betroffenen Person
2. Bestehendes Vertrags-/Anfrageverhältnis
3. Berechtigtes Interesse des Werbetreiben, das die schutzwürdigen Interessen des Betroffenen überwiegt
4. §7 UWG regelt die Zulässigkeit unterschiedlicher Kontaktwege

Vielen Dank für Ihre Aufmerksamkeit
Gibt es etwa noch Fragen????