Datensicherheit

Vorlesung 6: 19.01.2026

Wintersemester 2025/2026 h_da

Heiko Weber, Lehrbeauftragter

Teil 2: Datensicherheit
Themenübersicht der Vorlesung

1. Einführung / Grundlagen / Authentifizierung & Autorisierung
2. Kryptografie / Verschlüsselung & Signaturen / Vertrauen / Blockchain
3. Softwaresicherheit / Schadsoftware
4. Evaluation / Netzwerksicherheit / TLS / PGP & S/MIME / Firewalls & Netzwerksegmentierung
5. Hacking / Phishing / Einführung in den Datenschutz / Anonymität / Darknet
6. **Datenschutzgesetze / Technische & Organisatorische Maßnahmen**
7. **Organisationssicherheit / Managementsysteme / Zusammenfassung**

Geschichte des Bundesdatenschutzgesetzes

1970: hessisches Landesdatenschutzgesetz als erstes Datenschutzgesetz der Welt
1974: US Privacy Act
1977: erstes Bundesdatenschutzgesetz
1981: alle Bundesländer verfügen über ein Landesdatenschutzgesetz
1983: Volkszählungsurteil des BVerfG > „Recht auf informationelle Selbstbestimmung“
1990: zweites Bundesdatenschutzgesetz
1995: EU-Datenschutz-Richtlinie (95/46/EG)
2001: Novellierung des Bundesdatenschutzgesetzes
2003: erster europäischer Datenschutzbeauftragter
2005: Informationsfreiheitsgesetz > **Anpassungen am BDSG**
2006: Mittelstandsentlastungsgesetz > **Anpassungen am BDSG**
2008: Lidl- und Telekom-Datenschutz-Skandale **> Anpassungen am BDSG**
2009: Datenschutz in EU-Grundrechte-Charta
2016: Datenschutz-Grundverordnung (DSGVO) – anzuwenden seit 25.5.2018
2018: BDSG-neu

Die Nutzung personenbezogener Daten ist grundsätzlich verboten

außer, wenn es eine rechtliche Erlaubnis dafür gibt (z. B. im BDSG oder der DSGVO)

oder

wenn der Betroffene zur Nutzung seiner personenbezogenen Daten eingewilligt hat

Datenschutz-Grundverordnung (DSGVO)

- EU-Datenschutzgesetz – keine Richtlinie
- einheitlicher(er) Datenschutz in der EU
- Öffnungsklauseln erlauben nationale Regelungen
- ersetzt das alte Bundesdatenschutzgesetz + weitere Regelungen
- wirksam und anwendbar seit dem 25.5.2018
- sehr allgemeines Gesetz (Grundverordnung)
- Spezialgesetze, wie z. B. die ePrivacy-Verordnung, sollen noch konkretisieren

Art. 32 Abs. 1 DSGVO: Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Grundsätze für die Verarbeitung personenbezogener Daten

- Rechtmäßigkeit
- Fairness und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Vertraulichkeit, Integrität, Verfügbarkeit
- Rechenschaftspflicht

§ 9 BDSG-alt - TOMs

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Konkretisierung der TOMs in Anlage zu § 9 Satz 1 BDSG-alt

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Konkretisierung der TOMs in Anlage zu § 9 Satz 1 BDSG-alt

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. **1. Zutrittskontrolle** …nen personenbezogene Daten verarbeitet oder genutzt werden, zu … verwehren (Zutrittskontrolle),
2. **2. Zugangskontrolle** …en genutzt werden können (Zugangskontrolle),
3. **3. Zugriffskontrolle** …tungssystems Berechtigten ausschließlich auf die ihrer … und dass personenbezogene Daten bei der Verarbeitung, Nutzung … ändert oder entfernt werden können (Zugriffskontrolle),
4. **4. Weitergabekontrolle** …ronischen Übertragung oder während ihres Transports oder ihrer … verändert oder entfernt werden können, und dass überprüft und … personenbezogener Daten durch Einrichtungen zur …
5. **5. Eingabekontrolle** …werden kann, ob und von wem personenbezogene Daten in … rnt worden sind (Eingabekontrolle),
6. **6. Auftragskontrolle** …ag verarbeitet werden, nur entsprechend den Weisungen des …
7. **7. Verfügbarkeitskontrolle** …ge Zerstörung oder Verlust geschützt sind …
8. **8. Trennungsgebot** …e Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Zutrittskontrolle

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)

- Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.
- geregelt in der Zutrittskontrollrichtlinie einer Organisation – Sicherheitszonen bestimmen das geforderte Sicherheitsniveau

umgesetzt durch:

- Schlüssel, Zutrittskarten, Wachpersonal
- Alarmanlagen, Videoüberwachung

Zugangskontrolle

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)

- Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden.

umgesetzt durch:

- Authentifizierung
- Verschlüsselung

Zugriffskontrolle

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle)

- Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können.

umgesetzt durch:

- Autorisierung, Rollen- und Berechtigungskonzepte
- Verschlüsselung, Datenträgervernichtung

Weitergabekontrolle

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)

- Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung und während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

umgesetzt durch:

- Firewalls, VPN, Content-Filter
- Verschlüsselung – insbesondere beim Transport

Eingabekontrolle

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

- Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können.

umgesetzt durch:

- Protokollierung und Protokollauswertung

Auftragskontrolle

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

- Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

umgesetzt durch:

- organisatorische Maßnahmen: Regeln, Richtlinien, Anweisungen
- Vertragsgestaltung und Kontrolle

Verfügbarkeitskontrolle

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

- Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

umgesetzt durch:

- Backups und Archivierung
- Redundanz
- Antivirenstrategien

Trennungsgebot

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

- Maßnahmen, die sicherstellen, dass Daten die zu unterschiedlichen Zwecken übermittelt wurden, auch getrennt verarbeitet werden.

umgesetzt durch:

- Mandantenfähigkeit
- Anonymisierung und Pseudonymisierung

Verschlüsselung

Satz 3 der Anlage zu § 9 Satz 1 BDSG-alt:
Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Technische Maßnahmen

- Verschlüsselung
- Authentifizierung
- Autorisierung, Rollen- und Berechtigungskonzepte
- Anonymisierung
- Pseudonymisierung
- Backups und Archivierung
- Redundanz
- Mandantenfähigkeit
- Antivirenstrategien
- Protokollierung
- Firewalls, VPN, Content-Filter
- Schlüssel, Zutrittskarten, Wachpersonal
- Alarmanlagen, Videoüberwachung

Organisatorische Maßnahmen

- Regeln, Richtlinien, Anweisungen
- Protokollauswertung
- Vertragsgestaltung und Kontrolle

- Schulung der personenbezogene Daten verarbeitenden Personen
- Awareness-Trainings

Awareness-Trainings

- Erklärung der geltenden Regeln
- Beispiele was schief gehen kann
- Hinweise auf besondere Gefahrensituationen
- Sensibilisierung der Beschäftigten

Beispiel: Zutrittskontrolle

- **Organisatorische Maßnahmen**
  - Zutrittskontrollrichtlinie
  - Einteilung der Büroflächen in Sicherheitszonen
  - Arbeitsanweisungen bezogen auf den Umgang mit Besuchern
  - Mitarbeiter-Schulung rund um Zutrittsregeln
  - regelmäßige Kontrollen der Effektivität der Maßnahmen
- **Technische Maßnahmen**
  - Zutrittskontrollsysteme
  - Badges zur Kennzeichnung der Besucher
  - Besucherbereiche in einer niedrigen Sicherheitszone

TOMs gemäß DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Zutrittskontrolle zu Verarbeitungsbereichen
- Zugangskontrolle zu Datenverarbeitungssystemen
- Zugriffskontrolle auf besondere Bereiche von Datenverarbeitungssystemen
- Trennung der Verarbeitung für unterschiedliche Zwecke
- Pseudonymisierung
- Verschlüsselung

Integrität (Art. 32 Abs. 1 lit. b DSGVO)
- Eingabekontrolle
- Weitergabekontrolle

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Verfügbarkeitskontrolle
- Belastbarkeit

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs und organisatorische Maßnahmen zur Gewährleistung der Sicherheit (Art. 32 Abs. 1 lit. d DSGVO)
- Datenschutz-Management
- Incident-Response-Management
- Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle

Belastbarkeit

- speziellere Anforderung, die zur allgemeinen Verfügbarkeits-Anforderung dazu kommt
- Systeme in denen personenbezogene Daten verarbeitet werden, sollen auch mit ungewöhnlichen Belastungen in gewissen Maßen umgehen können und die erforderlichen Funktionen aufrecht erhalten können.
- Belastbare Systeme sind so konzipiert, dass sie auch mit extremen Situationen umgehen können und zudem muss das zuständige Ops-Team auf ungewöhnliche Situationen schnell reagieren können.

umgesetzt durch:

- DDoS-Schutz, Intrusion Detection Systems, Intrusion Prevention Systems
- regelmäßige Notfall-Simulationen
- Etablierung von Prozessen zur Aufrechterhaltung des Betriebs (Business Continuity Management System)

Privacy by Design

Artikel 25 Abs. 1 DSGVO:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

analog zu „Security by Design“ (siehe Vorlesung 3 - Softwaresicherheit)

Privacy by Design - Umsetzung

In allen Phasen einer Datenverarbeitung müssen die Datenschutzanforderungen berücksichtigt werden. Das kann gut auf die Software-Entwicklungs-Phasen abgebildet werden.

Anforderungsanalyse

Kategorien von personenbezogenen Daten und Betroffenen
Zweck der Verarbeitung
Rechtsgrundlage der Verarbeitung, Intl. Datentransfers
Verantwortliche, Auftragsverarbeiter

Entwurf

Planung der TOMs
Rollen- und Berechtigungskonzept erstellen
Löschkonzept erstellen
Auftragsverarbeitungsverträge abschließen

Implementierung

Umsetzung der technischen Maßnahmen

Überprüfung

Überprüfung der technischen Maßnahmen

Installation + Abnahme

Umsetzung der organisatorischen Maßnahmen

Betrieb + Wartung

Umsetzung der organisatorischen Maßnahmen
Datenlöschung
Betroffenenrechte umsetzen
regelmäßige Kontrolle und Anpassung, falls erforderlich

Privacy by Default

(Datenschutz durch datenschutzfreundliche Voreinstellungen)

Artikel 25 Abs. 2 DSGVO:

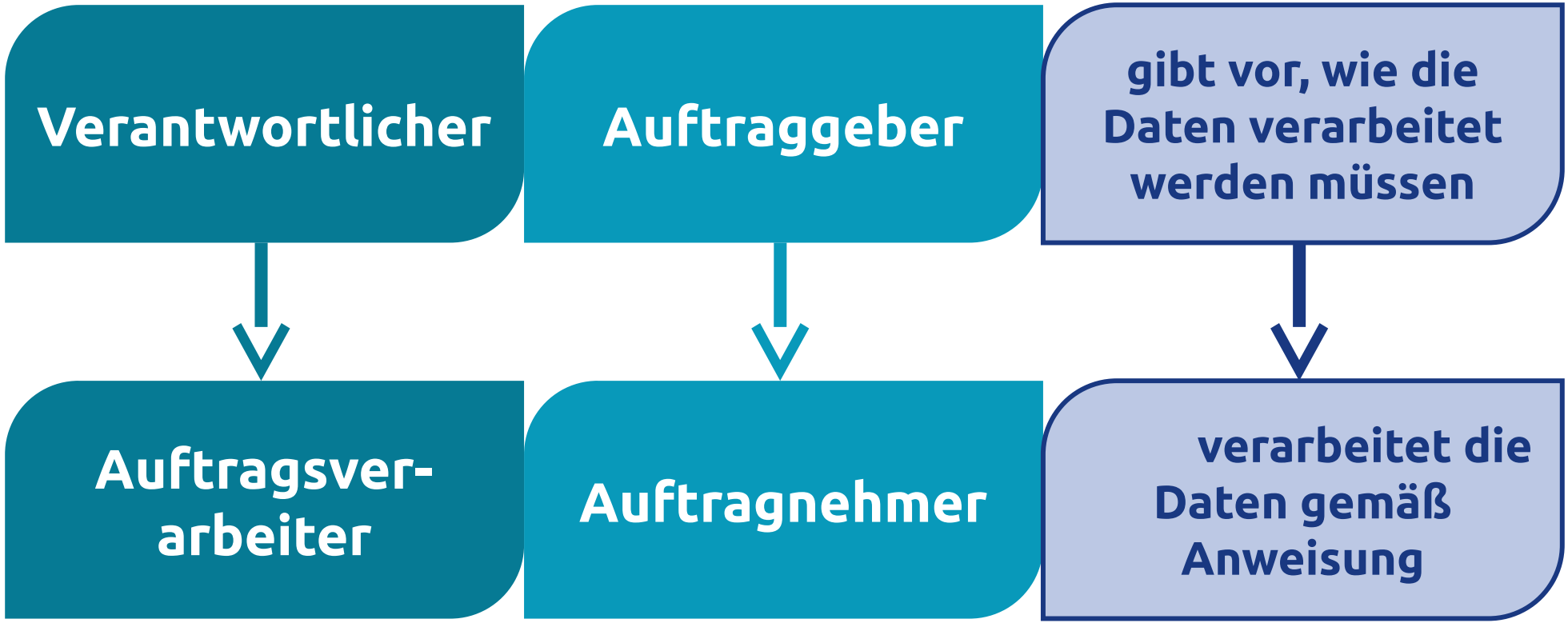
Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Verantwortlicher und Auftragsverarbeiter

Art. 4 DSGVO:

7. **„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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
8. **„Auftragsverarbeiter“** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Auftragsverarbeitung (Art. 28 DSGVO)



Auftragsverarbeitung

- Die Verantwortung für die personenbezogenen Daten bleibt beim Auftraggeber.
- Der Auftraggeber muss sicherstellen, dass er nur Auftragnehmer einsetzt, die den Datenschutz ausreichend umsetzen können.
- Der Auftraggeber bestimmt genau, was der Auftragnehmer mit personenbezogenen Daten machen darf.
- Der Auftragnehmer muss genau nach den Anweisungen des Auftraggebers handeln und darf selbst keine grundlegenden Entscheidungen fällen.

Beispiele für Auftragsverarbeitung

- Beratung für IT-Projekte
- die meisten Cloud-Dienste
- Outsourcing des Rechenzentrums
- Marketingaktionen, Kundenumfragen, Newsletterversand durch eine externe Agentur
- externe Akten- und Datenträgervernichtung
- externe Lohn- und Gehaltsabrechnung
- externe Buchhaltung
- auch Wartung von IT-Systemen

Rechtliche Grundlage für Auftragsverarbeitung

Auftraggeber muss sicherstellen, dass Auftragnehmer

1. nur nach seinen Anweisungen die Daten verarbeitet,

2. ausreichende Maßnahmen zum Schutz der Daten einsetzt,

3. in einem Land mit ausreichend hohem Datenschutzniveau ist.

ODER

3. vertraglich das ausreichend hohe Datenschutzniveau zusichert.

2. Auftraggeber muss sicherstellen, dass Auftragnehmer ausreichende Maßnahmen zum Schutz der Daten einsetzt

Anlage: TOMs
(Technische & Organisatorische Maßnahmen)

gemäß Art. 32 DSGVO

Probeklausur

- Im Moodle und auf der Webseite (https://weber-vorlesung.de/) befindet sich eine Probeklausur.
- Diese Probeklausur deckt den Teil 2 (Datensicherheit) der Vorlesung ab. Sie entspricht im Umfang und in der Art der Aufgaben der echten Klausur.
- Die Probeklausur gehen wir komplett am 26.01.2026 in der Vorlesung durch.