Hochschule Aalen

IT-Recht

Hochschule Aalen
Sommersemester 2024

Jana Thieme
Dipl.-Jur. Univ.
jana.thieme@hs-aalen.de

Überblick über die gesamte Vorlesung

• Einführung in das juristische Denken und Arbeiten 1	15.03.2024
• Einführung in das juristische Denken und Arbeiten 2	22.03.2024
• Grundlagen des Vertragsrechts 1	05.04.2024
• Grundlagen des Vertragsrechts 2	12.04.2024
• Fälle zum Vertragsrecht	19.04.2024
• Datenschutzrecht 1	26.04.2024
• **Datenschutzrecht 2**	**03.05.2024**
• Urheberrecht 1	10.05.2024
• Urheberrecht 2	17.05.2024
• IT-Vertragsrecht 1	31.05.2024
• IT-Vertragsrecht 2	07.06.2024
• Onlinerecht	14.06.2024
• Übungsklausur	21.06.2024
• Durchsprache Übungsklausur	28.06.2024

Datenschutz

Grundlagen und Aktuelles

Wie funktioniert Datenschutz?

Wie funktioniert Datenschutz?

- Datenschutzgrundsätze
- Betroffenenrechte
- Technische und organisatorische Maßnahmen (TOM)
- Aktuelle Themen
  - ✓ Datentransfer ins Ausland
  - ✓ Cookies & Tracking
  - ✓ Gesundheitsdatenschutz

Datenschutzgrundsätze, Art. 5 DSGVO

Alles ist verboten...

… es sei denn, es ist ausdrücklich erlaubt!

(sog. „Verbot mit Erlaubnisvorbehalt“)

… im „normalen“ Leben ist es genau umgekehrt!

Datenschutzgrundsätze, Art. 5 DSGVO

Erlaubnis z. B. aus:

- Einwilligung
- Vertrag
- Gesetz, z. B.:
  - ✓ früher: § 26 BDSG (Beschäftigtendaten)
  - ✓ Handels- und Steuerrecht (Aufbewahrungsfristen)
  - ✓ uvm.
- berechtigtes Interesse

Datenschutzgrundsätze, Art. 5 DSGVO

Exkurs: Einwilligung des Betroffenen

Mit der Einwilligung lässt ein Mensch erkennen, dass die Verwendung seiner Daten in einem bestimmten Kontext mit seinem Wertesystem vereinbar ist.

- Bedingungen für die Einwilligung, Art. 7 DSGVO
- Informationspflichten, Art. 13, 14 DSGVO

Einwilligung des Betroffenen

Formulieren Sie eine elektronische Einwilligungserklärung, die die Anforderungen der DSGVO erfüllt, anhand eines frei gewählten Beispiels!

Lösung: Einwilligung des Betroffenen

Ich bin bis auf Widerruf damit einverstanden, dass meine personenbezogenen Daten von der ... zu folgenden Zwecken verarbeitet, (sowie an ... übermittelt und dort ebenfalls zu folgenden Zwecken verarbeitet werden):

... (Art der pbD, Zweck, Rechtsgrundlage)

Die Daten werden für folgenden Zeitraum ... gespeichert und anschließend gelöscht.

Ich bin darauf hingewiesen worden, dass die Verarbeitung meiner personenbezogenen Daten auf freiwilliger Basis erfolgt. Ferner bin ich darauf hingewiesen worden, dass ich mein Einverständnis verweigern bzw. jederzeit mit Wirkung für die Zukunft widerrufen kann. Im Fall des Widerrufs dürfen mit dem Zugang meiner Widerrufserklärung die entsprechenden Daten zukünftig nicht mehr für den widerrufenen Zweck verarbeitet werden und sind ggf. unverzüglich zu löschen. Aus der Verweigerung der Einwilligung oder einem Widerruf entstehen mir keine Nachteile.

Meine Widerrufserklärung werde ich richten an: ... (verantwortliche Stelle)

Ich bin außerdem berechtigt, hier jederzeit Auskunft, ggf. Berichtigung, Löschung oder Einschränkung der Verarbeitung meiner gespeicherten personenbezogenen Daten zu verlangen. Darüber hinaus habe ich das Recht auf Übertragung meiner personenbezogenen Daten in einem maschinenlesbaren Format.

Ich bin darauf hingewiesen worden, dass ich unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde habe, wenn ich der Ansicht bin, dass die Verarbeitung der mich betreffenden personenbezogenen Daten gegen geltende Gesetze verstößt.

Der Datenschutzbeauftragten der ... ist erreichbar unter: Kontaktdaten des Datenschutzbeauftragten

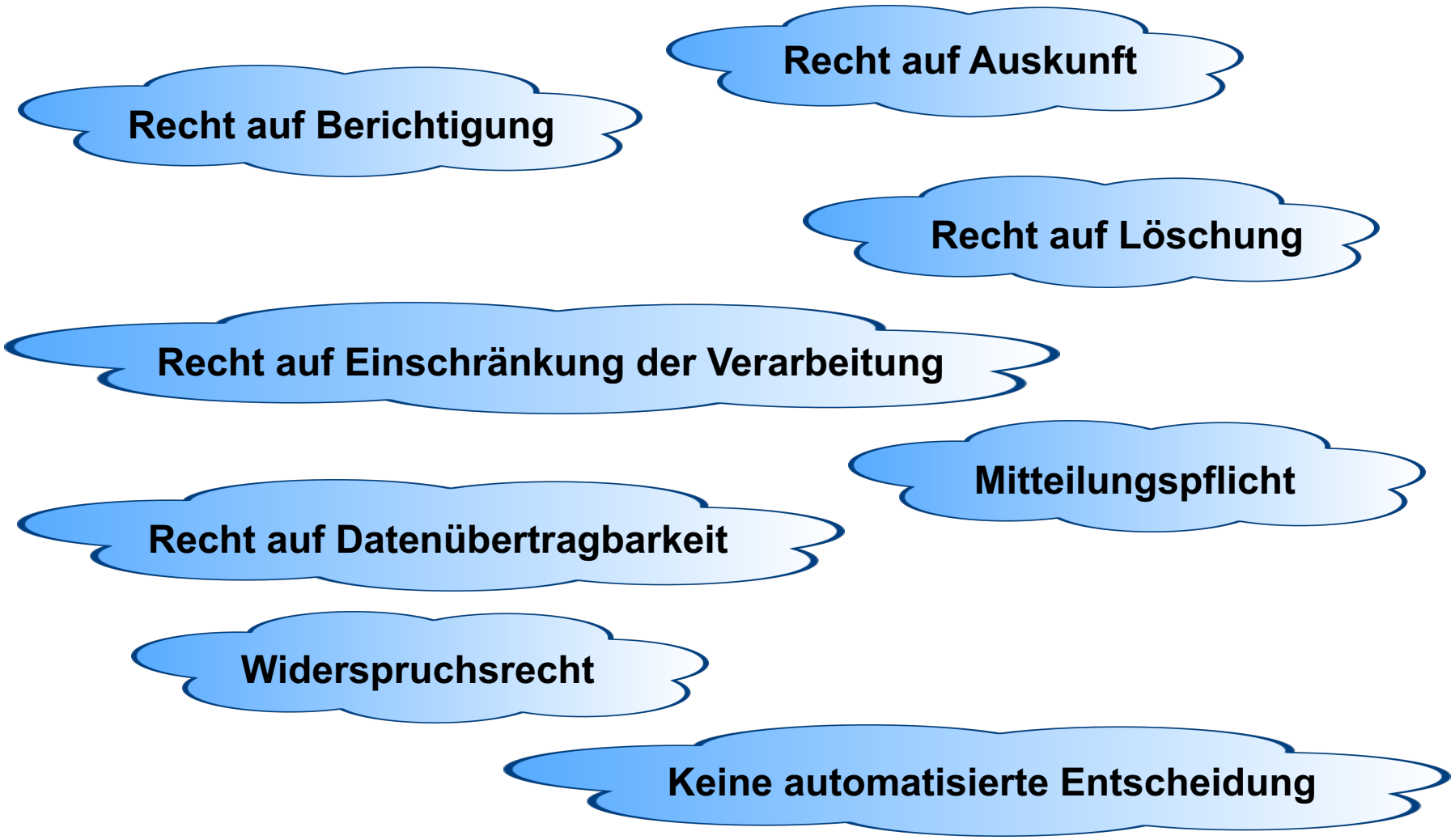
<u>Elektronische Einwilligungserklärung:</u>

In der Regel sollte eine Einwilligung in schriftlicher Form erfolgen. Für Online-Formulare darf von der Schriftform abgewichen werden, allerdings muss hier darauf geachtet werden, dass explizit ein Optionshäkchen gesetzt werden muss, damit die Einwilligung gültig ist (es darf keine Vorauswahl getroffen sein und kein implizites Einverständnis ("Mit dem Abschicken von ... bin ich einverstanden mit....") eingeholt werden.

******Die Einwilligung muss dokumentiert werden und jederzeit vom Betroffenen abgefragt werden können.******

Datenschutzgrundsätze, Art. 5 DSGVO

Betroffenenrechte, Art. 15 ff. DSGVO



Datenschutzgrundsätze, Art. 5 DSGVO

Schutzziele der Informationssicherheit

Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen

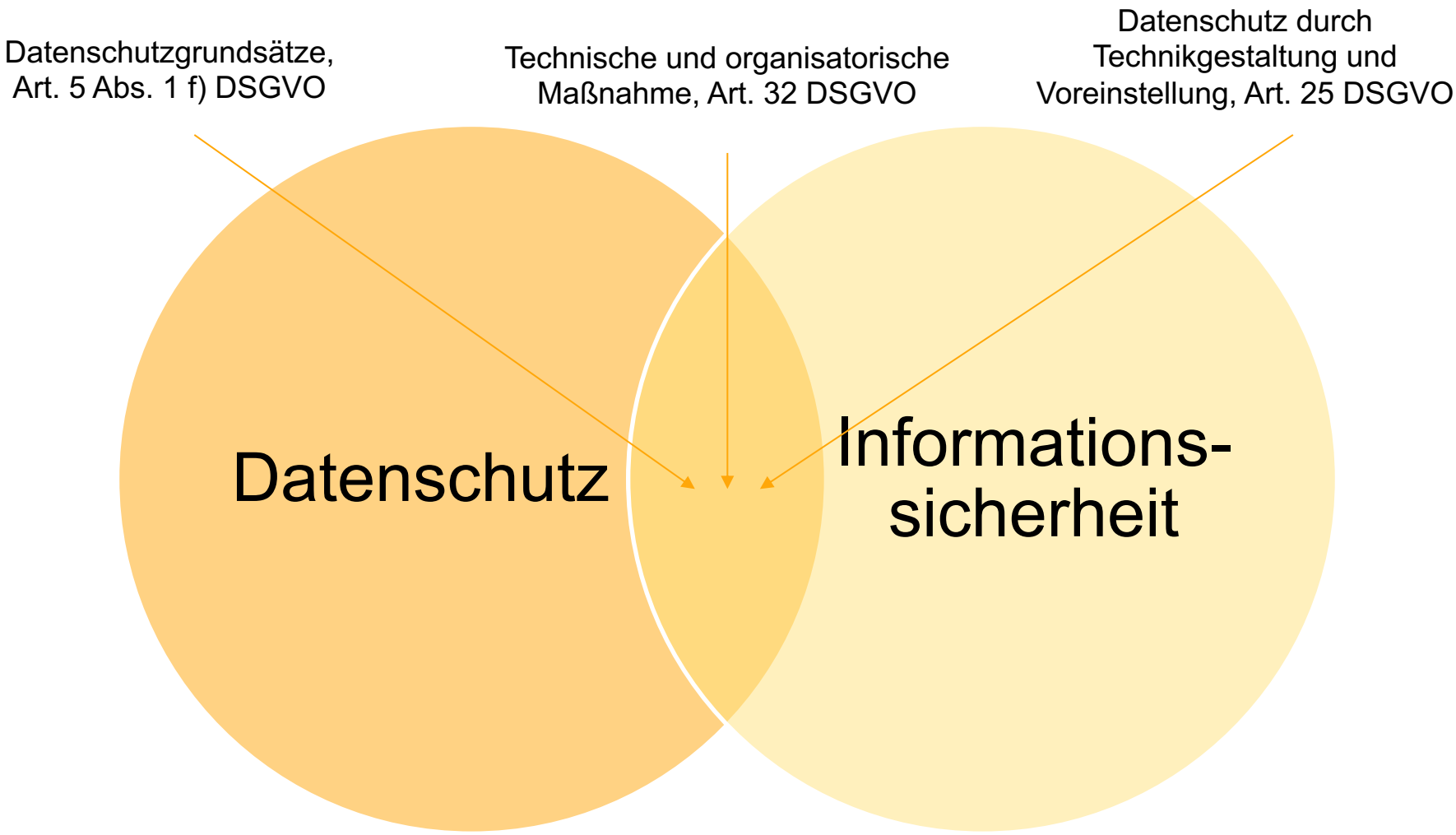
Informationssicherheit & Datenschutz

Datenschutz	Informationssicherheit
im Fokus: die einzelne Person	im Fokus: das Unternehmen
geschützt werden: Persönlichkeitsrechte	geschützt werden: Unternehmenswerte (Know-How etc.)
Risiko: Verletzung der Rechte betroffener Personen	Risiko: Nichtverfügbarkeit, Verlust, Zerstörung, Missbrauch von Unternehmensdaten
rechtliche Grundlage: DSGVO, BDSG etc.	rechtliche Grundlage: TMG, TKG etc.
Verantwortlich: Geschäftsführung	Verantwortlich: Chief Information Security Officer (CISO)

Informationssicherheit & Datenschutz

Datenschutz	Informationssicherheit
Grundsatz der Datensparsamkeit	Redundante Datensicherung
Recht auf informationelle Selbstbestimmung	Nachvollziehbarkeit von Zugriffen
Transparenz	Geheimhaltung von Schutzmechanismen und Informationen
Inhalte von Daten	Transport von Daten
Betroffene	Systembetreiber

Informationssicherheit & Datenschutz

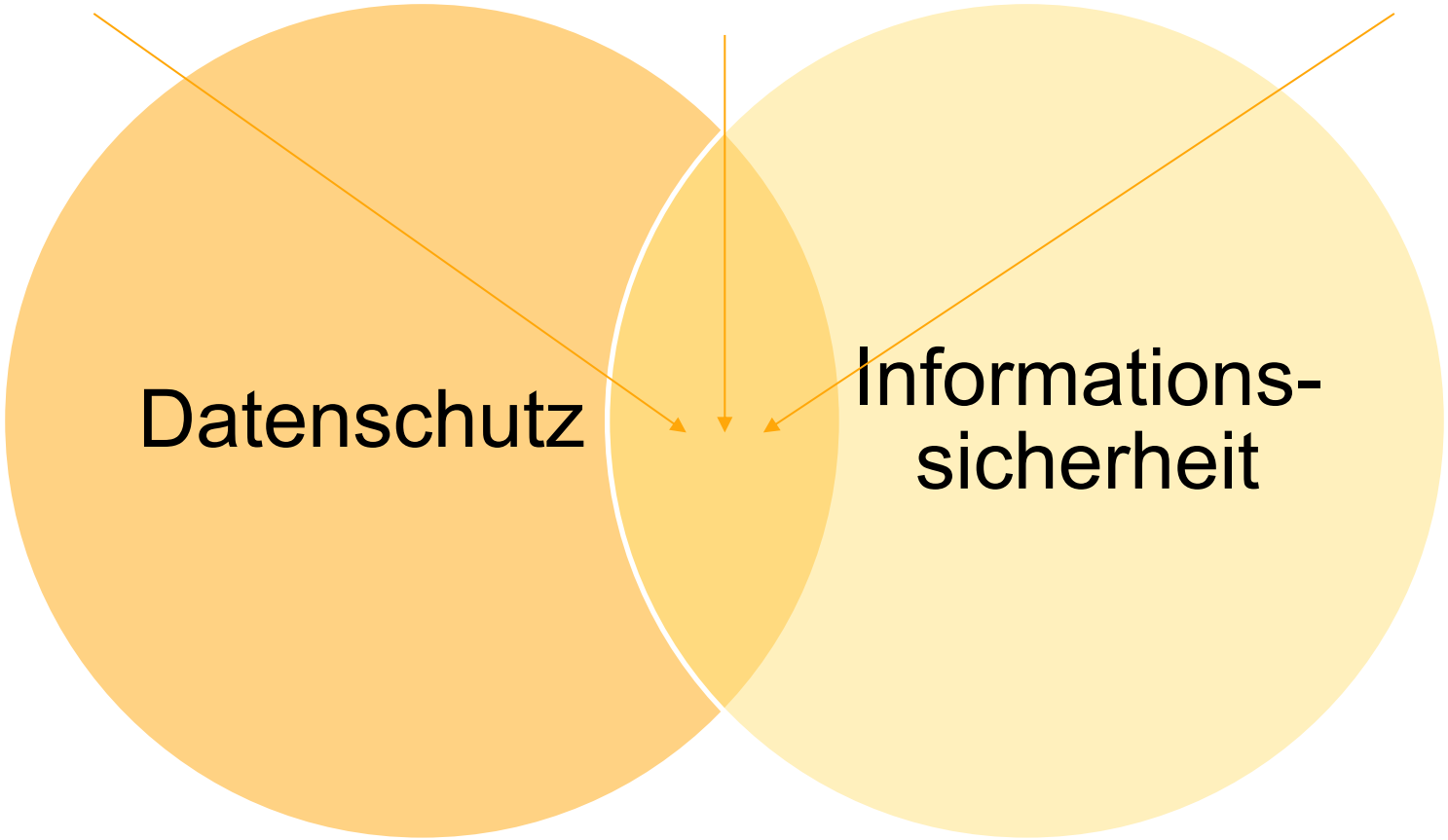


Informationssicherheit & Datenschutz

Datenschutzgrundsätze, Art. 5 Abs. 1 f) DSGVO

Technische und organisatorische Maßnahme, Art. 32 DSGVO

Datenschutz durch Technikgestaltung und Voreinstellung, Art. 25 DSGVO



Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

- Technische Maßnahmen sind organisatorischen vorzuziehen
- Die Maßnahmen müssen dem identifizierten Risiko angemessen sein
- Die Maßnahmen müssen dem Stand der Technik entsprechen
- Bei der Risikobewertung kommt es auf die betroffene Person an, nicht auf das Unternehmen

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

- **Pseudonymisierung** personenbezogener Daten
- **Verschlüsselung** personenbezogener Daten
- Gewährleistung der **Vertraulichkeit** der Systeme und Dienste
- Gewährleistung der **Integrität** der Systeme und Dienste
- Gewährleistung der **Verfügbarkeit** der Systeme und Dienste
- Gewährleistung der **Belastbarkeit** der Systeme und Dienste
- **Wiederherstellung** der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und **Evaluierung** der Wirksamkeit der vorgenannten Maßnahmen

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Pseudonymisierung

die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können

- Trennung von Kundenstammdaten und Kundenumsatzdaten
- Verwendung von Personal- oder Kundennummern statt Namen

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Verschlüsselung (z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport):

- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Vertraulichkeit

- Zutrittskontrolle (Gebäude)
- Zugangskontrolle (Datenverarbeitungsanlagen)
- Zugriffskontrolle (spezifische Daten)
- Weitergabekontrolle (Transport von Daten)
- Trennungskontrolle (Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Integrität

- Eingabekontrolle (ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind)
- organisatorische und technische Absicherung von Protokollierungsmaßnahmen, Protokoll-Auswertungen/Revision etc.

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Verfügbarkeit

- Verfügbarkeitskontrolle (Notfallplan, Brandschutz, Stromausfall, Datensicherung etc.)
- Auftragskontrolle (sorgfältige Auswahl des Auftragnehmers, eindeutige Vertragsgestaltung etc.)

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Belastbarkeit

- bezieht sich insbes. auf Speicher-, Zugriffs- und Leitungskapazitäten

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen:

- Backup-Konzept
- Redundante Datenspeicherung
- Cloud-Services
- Doppelte IT-Infrastruktur

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen:

- Sicherheitskonzept
- Prüfungen des DSB, der IT-Revision
- Externe Prüfungen, Audits, Zertifizierungen

Technische und organisatorische Maßnahmen (TOM), Art. 32 DSGVO

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen:

- Sicherheitskonzept
- Prüfungen des DSB, der IT-Revision
- Externe Prüfungen, Audits, Zertifizierungen

Weiterführende Informationen

Der Landesbeauftragte für den Datenschutz Baden-Württemberg
https://www.baden-wuerttemberg.datenschutz.de

Links:

- Bundesamt für Sicherheit in der Informationstechnik
  https://www.bsi.bund.de/DE/Home/home_node.html
- Working Papers der Art. 29-Gruppe
  https://www.datenschutz-hamburg.de/datenschutz-fuer-firmen-und-behoerden/das-neue datenschutzrecht/working-papers-art-29.html
- Datenschutzkonferenz (DSK)
  https://www.lda.bayern.de/de/datenschutz_eu.html
- Zentralarchiv für Tätigkeitsberichte des BDSB und LDSB
  https://www.thm.de/zaftda

Hilfsmittel:
ISO- und DIN-Normen zu Informationssicherheit und Datenschutz
(z. B. ISO 27001, 19600)

Hochschule Aalen

IT-Recht

Hochschule Aalen
Sommersemester 2024

Jana Thieme
Dipl.-Jur. Univ.
jana.thieme@hs-aalen.de