Universität Bremen

Grundlagen der Angewandten Informatik (VAK: 03-IBGA-AI)

Introduction to Ethical, Legal and Social Aspects of Computing

Prof. Dr. Andreas Breiter
15.5.2025

Zentrale Fragen der Veranstaltung

Was bedeutet digitale Transformation für verschiedene Anwendungsfelder und ihre Organisation?	• Unser Fokus: Was ist der Unterschied zwischen IT-gestützter, organisationaler Transformation vs. digitale Transformation?
Wie kann man digitale Transformationsprozesse empirisch erforschen und gestalten?	• Unser Fokus: Wie lassen sich Prozesse erfassen, modellieren und verbessern?
Welche gesetzlichen Rahmenbedingungen prägen digitale Transformationsprozesse?	• Unser Fokus: Datenschutz, Urheberrecht
Welche theoretischen Konzepte erlauben eine kritische Auseinandersetzung mit digitalen Transformationsprozessen?	• Unser Fokus: Social Stud… Data/Algorithm Studies, …

Schaut bitte die Videos VOR der Sitzung am 3.6.25 an!

Ablauf der weiteren Sitzungen

Termin	Themen
15.5.	BLOCK 2: Rechtsgebiete: Datenschutz, Informationssicherheit und Mitbestimmung
22.5.	BLOCK 2: Rechtsgebiete: Urheberrecht
29.5.	Vorlesung fällt aus (Christi Himmelfahrt)
5.6.	BLOCK 2: Fragestunde zur e-Klausur (digital mit Prof. Kirchner-Freis)
12.6.	e-Klausur zu den Rechtsgebieten => Anmeldung!
19.6.	BLOCK 3: Sozio-technische Systeme und Aktanten
26.6.	BLOCK 3: Sozio-technische Systeme und Affordances
3.7.	BLOCK 3: Sozio-technische Systeme und Akzeptanzmodelle
10.7.	BLOCK 3: Ethik

Übersicht zur e-Klausur

- 2 Videos (von Prof. Iris Kirchner-Freis eine Auswahl aus eGeneral Studies) zum Selbststudium:
  - **Urheberrecht**: https://oncourse.uni-bremen.de/course/view.php?id=33&chapter=1&selected_week=4
  - **Datenschutzrecht**: https://oncourse.uni-bremen.de/course/view.php?id=33&chapter=9&selected_week=28
- Auf Basis dieser Videos ist die e-Klausur erstellt. Wer die Videos versteht, kann die e-Klausur sehr gut lösen.
- Format: Geschlossene Fragen (ja/nein) und 2 offene Fragen anhand eines Szenarios (Urheberrecht und Datenschutzrecht)
- Dauer 1 Stunde, 12.6.25, 10-11 bzw. 11:15-12:15 Uhr (Eintragung über stud.IP Gruppen), im Testcenter der Universität Bremen, auf dem Boulevard neben der SuUB

→ Am 5.6.25 kommt Prof. Kirchner-Freis (per Zoom) in die Veranstaltung und beantwortet eure Fragen (wird im Tutorium vorbreitet): https://uni-bremen.zoom-x.de/j/66527078966?pwd=KdTkDQURTxBA1NIupB7sHLzRHax7iC.1

Datenschutz = Schutz von Daten?

Im Sinne dieser Verordnung bezeichnet der Ausdruck:
1. „personenbezogene Daten“ 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
DSGVO § 4 (1)

Datenschutz als Grundrecht: Das Volkszählungsurteil des BVerfG (1983)

„Das **Persönlichkeitsrecht** umfaßt [...] auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. [...] Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes."

„Mit dem Recht auf **informationelle Selbstbestimmung** wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß.[…] Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"

Art. 1 Abs. 1
Art. 2 Abs. 1
GG

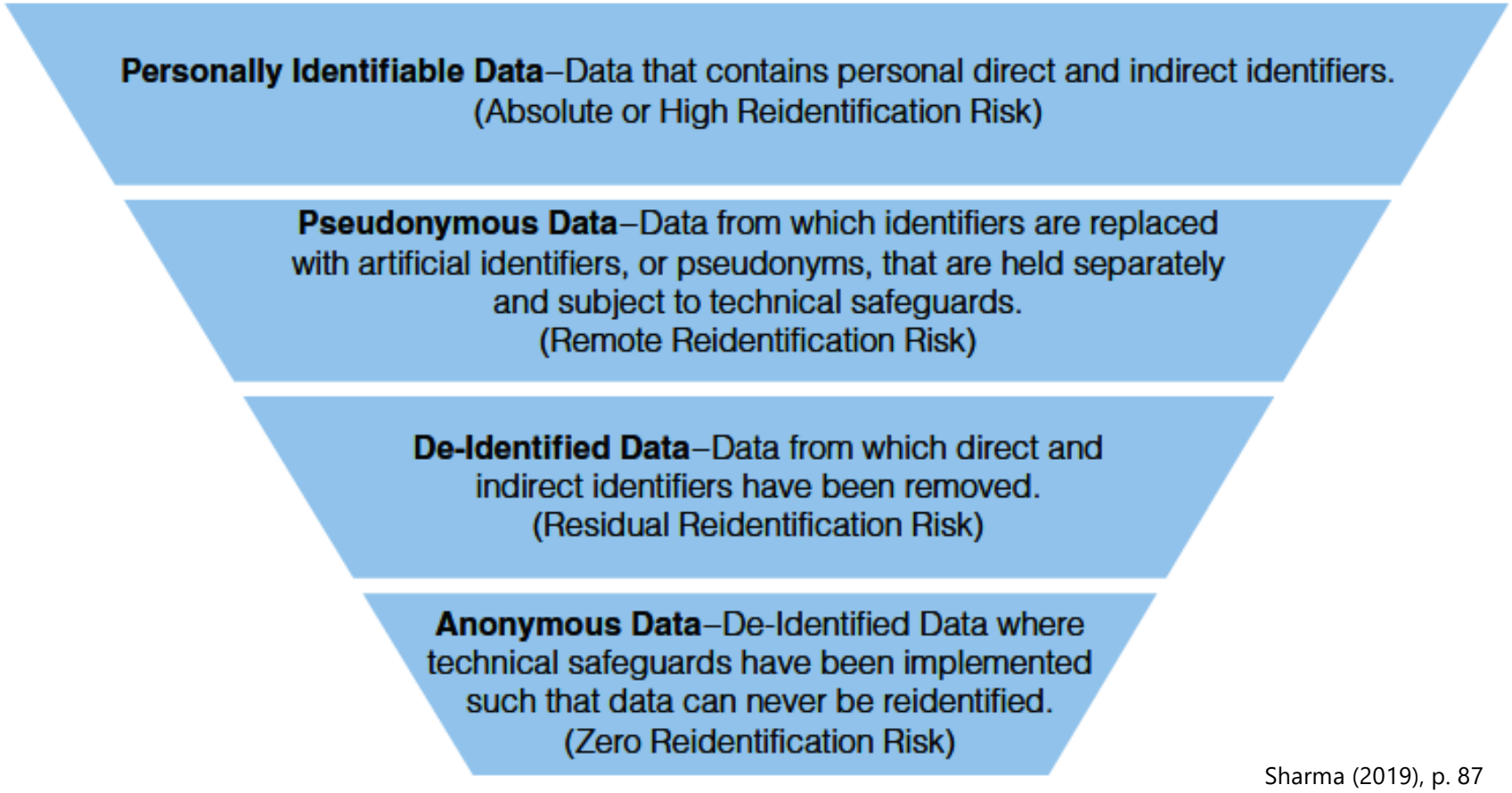
1. Grundprinzip: Verbot mit Erlaubnisvorbehalt

→Rechtfertigungsmöglichkeiten:

→1. Einwilligung der/des Betroffenen als Ausdruck der individuellen informationellen Selbstbestimmung
(Art 6 Abs 1, a DSGVO)

→2. Gesetzliche Grundlagen als Ausdruck der kollektiven informationellen Selbstbestimmung
(z.B. Art 6 Abs 1, b-f DSGVO, Art. 88 DSGVO, BDSG-neu, Landesgesetze, bereichsspezifische Gesetze)

Hierarchie schutzwürdiger Daten



Sharma (2019), p. 87

Bereichsspezifische Regelungen (Beispiele)

- → Ausländerzentralregistergesetz
- → Bundesverfassungsschutzgesetz
- → Bundesgrenzschutzgesetz
- → Postgesetz
- → **Schulgesetze (der Länder)**
- → Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)
- → Sozialgesetzbuch
- → **Betriebsverfassungsgesetz**
- → **Personalvertretungsgesetze (der Länder)**
- → Abgabenordnung
- → Zivilprozessordnung
- → Gewerbeordnung
- → Straßenverkehrsgesetz
- → Melderechtsrahmengesetz
- → Bundeszentralregistergesetz

Gesetz zum Datenschutz im Schulwesen (Schuldatenschutzgesetz) in der FHB

§12 Schülerverzeichnis

→ (1) Zur Überwachung der Schulpflicht und zur Vorbereitung, Durchführung und Auswertung schulorganisatorischer Maßnahmen sowie für schulstatistische und berufsvorbereitende Zwecke können beim Senator für Bildung und Wissenschaft und beim Magistrat Bremerhaven nachstehende Daten in automatisierten Dateien verarbeitet werden:

- 1. Bei allgemeinbildenden Schulen Name, Geburtsdatum, Adressdatum, Geschlecht, Staatsangehörigkeit, Muttersprache, Aussiedlereigenschaft und Einschulungsdatum der Schülerin oder des Schülers und die von ihm oder ihr besuchte Klasse sowie von den Erziehungsberechtigten Name und Adressdatum;
- 2. bei beruflichen Schulen darüber hinaus die Daten des Ausbildungsberufes, des betrieblichen Ausbildungsbeginns und des Ausbildungsendes der Schülerin oder des Schülers.

zuletzt geändert durch Geschäftsverteilung des Senats vom 20.10.2020 (Brem.GBl. S. 1172)

Auftragsdatenverarbeitung

- → Verarbeitung personenbezogener Daten im Auftrag durch eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle (Art. 4 Abs. 8 DSGVO).
- → Muss so organisiert sein und mit solchen technischen Mitteln erfolgen, dass die Datenschutzanforderungen der DSGVO insgesamt eingehalten werden und der Schutz der Rechte der betroffenen Person gewährleistet wird (Art. 28 Abs. 1 DSGVO).
- → Durch den Auftragsverarbeiter dürfen keine weiteren Auftragsdatenverarbeiter (Subunternehmer) ohne Zustimmung des Verantwortlichen eingeschaltet werden (Art. 28 Abs. 2 DSGVO). Auch wenn der Verantwortliche zugestimmt hat, bleibt der ursprüngliche Verarbeiter vollständig haftbar (Art. 28 Abs. 4 S. 2 DSGVO).
- → Zwischen ursprünglichem Verarbeiter und jedem weiteren Verarbeiter gelten die gleichen Standards wie im Verhältnis zwischen dem Verantwortlichen und dem ursprünglichen Verarbeiter (Art. 28 Abs. 4 S. 1 DSGVO).
- → Drittstaaten: gilt auch, wenn Auftragsverarbeiter, der nicht in der EU niedergelassen ist, personenbezogene Daten von Personen verarbeitet, solange diese Daten in der EU gesammelt werden. Zudem auch geregelt wie mit Drittstaaten umzugehen ist (gleiches Datenschutzniveau muss gewährleistet sein).

Hoeren 2020: Skript Internetrecht, https://www.itm.nrw/wp-content/uploads/skript-internetrecht-juli-2020.pdf

Datenschutz: Zuständigkeiten in Deutschland

BDSG:
→ Öffentliche Verwaltung des Bundes
→ Nicht-öffentlicher Bereich (Privatwirtschaft)

Aufsicht:
→ Bundesbeauftragter
→ Aufsichtsbehörden (Regierungspräsidium / Bezirksregierung, tw. Landes-DSB)

LDSGe
→ Öffentliche Verwaltung der Länder und der Kommunen

Aufsicht:
→ Landesdatenschutzbeauftragte

Betriebe:
- Betriebliche DSB

Verwaltungen:
- Behördliche DSB

Aufgabe Datenschutzbeauftragte (Art. 39 DSGVO)

- → Pflicht bei öffentlichen Stellen! Bei Unternehmen ab 20 Mitarbeiter:innen (oder bei umfangreicher Verarbeitung besonderer Datenkategorien).
- → Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten;
- → Sicherstellung der Erstellung eines Verzeichnisses aller Verarbeitungstätigkeiten
- → Überwachung der Einhaltung dieser Verordnung sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- → Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;
- → Zusammenarbeit mit der Aufsichtsbehörde;
- → Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Datenschutzfolgeabschätzung (DSFA)

→Verbindlich für zahlreiche öffentliche und nicht-öffentliche Stellen, die Daten erheben, verarbeiten und nutzen

→Maßgebliches Ziel: systematische Vorabbewertung von Risiken für die Rechte und Freiheiten der Betroffenen, die einzelne Verarbeitungsvorgänge mit sich bringen.

→Auch Strategien entwickeln, die die Verminderung von Risiken in jedem Einzelfall zum Ziel haben

Elemente einer DSFA

1. exakte **Beschreibung der geplanten Verarbeitungsvorgänge** und der jeweiligen Verarbeitungszwecke sowie etwaiger berechtigter Interessen des Verantwortlichen
2. Evaluierung von **Notwendigkeit und Verhältnismäßigkeit** der Erhebung personenbezogener Daten bezogen auf den jeweiligen Zweck
3. Evaluierung von **Risiken** für die Freiheiten sowie Rechte der Betroffenen
4. geplante **Abhilfemaßnahmen**, mit deren Hilfe die Risiken bewältigt werden können (Garantien, Sicherheitsvorkehrungen, Verfahren)

Checkliste: https://www.datenschutz.org/folgenabschaetzung/

Technisch-organisatorische Maßnahmen (TOM)

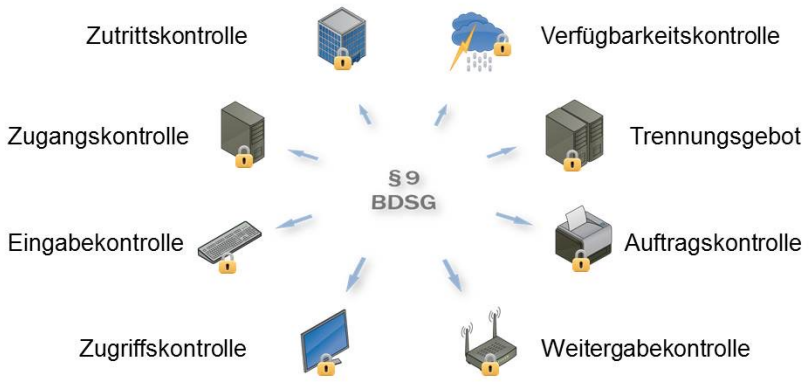
→TOM gemäß §32 DSGVO:

→die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

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

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

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



TOMs im Detail

Zutrittskontrolle:

- Physischer Zutritt zu verhindern (elektronische Zugangssysteme oder Pförtner).

Zugangskontrolle:

- Kein Zugriff auf Daten für Dritte (Verschlüsselungen, Mehr-Faktor-Authentifizierungen)

Zugriffskontrolle:

- Berechtigungskonzepte verhindern, dass unbefugte Dritte Schreib- oder Lesezugang bzw. Löschmöglichkeit erhalten.

Weitergabekontrolle:

- Verschlüsselungen verhindern, dass sensible Daten auch in der *Übertragung geschützt sind

Eingabekontrolle:

- Erfassung aller Zugriffe auf die Daten durch Protokollierungs-Software

Verfügbarkeitskontrolle:

- Schutz vor Verlusten oder Angriffen (Firewalls und Backups, schnelle Wiederherstellung

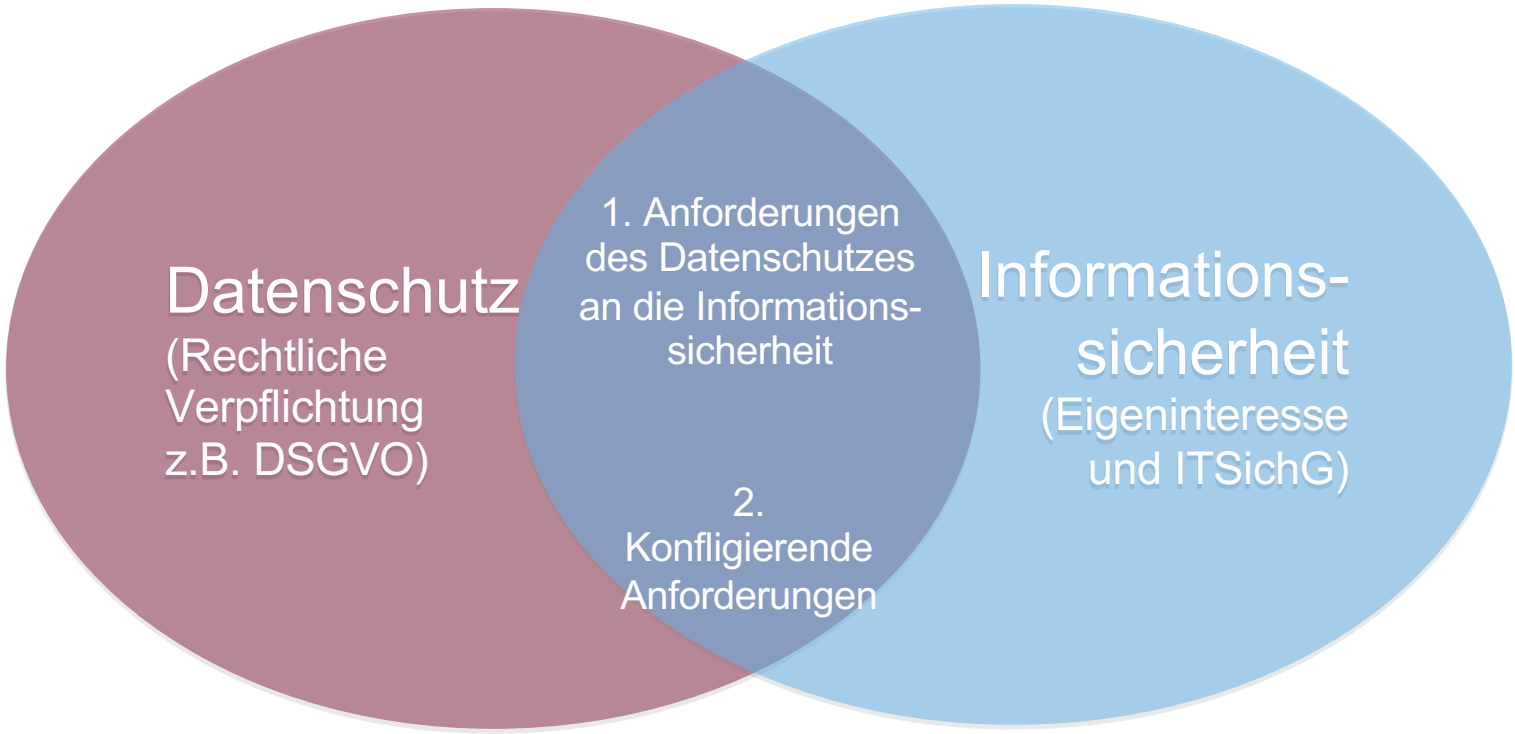
Trennungsgebot:

- Nachweis, dass für unterschiedliche Zwecke erhobene Daten nur für den jeweiligen Erhebungszweck verwendet werden.

Auftragskontrolle:

- AV-Verträge regeln die Datenverarbeitung durch auf diese Weise befugte Dritte.

Verhältnis zwischen Datenschutz und Informationssicherheit



Zentrale Ziele der Informationssicherheit

Sachziel	**Schutz gegen …**
Verfügbarkeit	Ausfall
Integrität	unerwünschte Veränderung
Vertraulichkeit	unbefugte Einsichtnahme
Authentizität	Täuschung (Sender)
Rechtsverbindlichkeit	Täuschung (Inhalt)
Anonymität	Identifizierung
Pseudonymität	Namentliche Identifizierung
Abrechenbarkeit	Betrug
Unbeobachtbarkeit	Protokollierung
Nicht-Vermehrbarkeit	„Viren“-Aktivitäten

Kersten & Wolfenstetter 2000, Pohl (2019)

Nachhaltigkeit: Sustainable Development Goals

https://en.unesco.org/sites/default/files/sdgs_poster_new1.png

Interessensvertretung

In Betrieben mit in der Regel mindestens fünf ständigen wahlberechtigten Arbeitnehmern, von denen drei wählbar sind, werden **Betriebsräte** gewählt. Dies gilt auch für gemeinsame Betriebe mehrerer Unternehmen. (§ 1 BetrVG)

In den Verwaltungen des Landes Bremen und der Stadtgemeinden Bremen und Bremerhaven und den sonstigen nicht bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts im Lande Bremen sowie den Gerichten des Landes Bremen werden **Personalvertretungen** gebildet. (§ 1 BremPersVG)

Warum ist dies für die Digitalisierung wichtig?

→ **1. Mitbestimmungsrechte des Betriebsrates**

→ Initiativ- und Zustimmungsverweigerungsrecht (z.B.

- Sozialer Bereich (Ordnung des Betriebes, Arbeitszeit, Einführung und Anwendung technischer Kontrollgeräte, betriebliches Vorschlagswesen, Gruppenarbeit, Urlaubsplan usw.) (§ 87)
- Personelle Einzelmaßnahmen (z.B. Einstellung, Eingruppierung, Umgruppierung und Versetzung) => Verweigerung bei Verstoß gegen Gesetze/ Verordnungen/ Betriebsvereinbarungen u.e.m. (§ 99)
- Kündigung: Der Arbeitgeber hat die Gründe für die Kündigung mitzuteilen. Eine ohne Anhörung des Betriebsrats ausgesprochene Kündigung ist unwirksam. (§ 102)
- Sozialplan (§ 112)

Warum ist dies für die Digitalisierung wichtig?

→ **2. Rechtliche Einflussmöglichkeiten des Betriebsrats**

→ Rechtzeitige und umfassende Unterrichtung (§ 80 II bzw. § 90 I BetrVG)

- Pflichtenheft, Programmbeschreibungen, Übersicht der zu verarbeitenden personenbezogenen Daten und die Auswertungen

→ Mitbestimmungspflicht bei Einführung und Anwendung eines Systems (§ 87 I (6) BetrVG)

- Leistungs- und Verhaltenskontrolle,
- Gestaltung von Bildschirmarbeitsplätzen,
- Qualifikationsmaßnahmen.

→ Arbeits- und Gesundheitsschutz

- Psychische Belastungen (Stressfaktoren) (§ 87 I BetrVG)

Im betrieblichen Kontext: Arbeitnehmer:innen-Datenschutz

- → … soll im Allgemeinen die **Persönlichkeitsrechte**, im Besonderen das **Recht auf informationelle Selbstbestimmung der Arbeitnehmer:innen** vor Missbrauch bewahren.
- → Es gibt kein **Arbeitnehmer:innen-Datenschutzgesetz**. Stattdessen finden dezentral einzelne Regelungen in anderen Gesetzestexten (DSGVO, TMDDSG, BildSchVO usw.)
- → Arbeitgeber dürfen nur personenbezogene Daten erheben, die **für die Aufnahme, Beendigung oder Durchführung Ihres Beschäftigungsverhältnisses relevant** sind.
- → Die **heimliche Überwachung** von Telekommunikation, Aktivitäten am PC oder die heimliche Videoüberwachung durch den Arbeitgeber sind regelmäßig nicht zulässig.

https://www.datenschutz.org/arbeitnehmerdatenschutz/

Im betrieblichen Kontext: Rechte der Arbeitnehmer:innen

→ Allgemeines Auskunftsrecht des Betroffenen:
- Alle gespeicherten Daten – auch die Personalakte – jederzeit einsehbar.
- Die Inhalte muss der Arbeitgeber streng vertrauliche behandeln.

→ Recht auf Löschung, Berichtigung oder Sperrung:
- Betrifft falsche, widerrechtlich erhobene oder veraltete Daten – auch, wenn das Arbeitsverhältnis gelöst wird.

→ Recht auf aktive Zustimmung:
- Besondere personenbezogene Daten (Gesundheitsdaten, Informationen zu Sexualität, Ethnie oder Religion) dürfen zur Wahrung vom Arbeitnehmerdatenschutz nur unter eindeutiger Einwilligung Ihrerseits erhoben, verarbeitet und genutzt werden
- oder wenn diese frei und öffentlich für jeden zugänglich sind (etwa bei Facebook, Twitter).

→ Recht auf Zurückhaltung von sensiblen Daten:
- Beispiel Arbeitsunfähigkeit: keine Auskunft über den genauen Grund für die Krankschreibung

→ Recht zu „lügen“:
- Werden sensible Informationen erfragt, ohne verpflichtete Freigabe, kann die Beantwortung verweigert oder unwahre Antworten gegeben werden.

https://www.datenschutz.org/arbeitnehmerdatenschutz/

KI-Definition im EU AI Act

→ Art. 3 (1) "KI-System":

- ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach dem Einsatz Anpassungsfähigkeit zeigen kann, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können;

Der EU AI Act und die Bedeutung für den Datenschutz (Rollen)

→ Unterscheidungen:

- in der DSGVO zwischen Verantwortlichen und Auftragsverarbeitern
- Im AI Act zwischen verschiedenen Kategorien (Art. 3)
  - (3) "Anbieter" (Provider) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell für allgemeine Zwecke entwickelt oder ein KI-System oder ein KI-Modell für allgemeine Zwecke entwickeln lässt und es unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr bringt oder in Betrieb nimmt, unabhängig davon, ob dies entgeltlich oder unentgeltlich geschieht;
  - (4) "Bereitsteller“ (Deployer): eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System unter ihrer Aufsicht einsetzt, es sei denn, das KI-System wird im Rahmen einer persönlichen, nicht beruflichen Tätigkeit verwendet

Der EU AI Act in der Übersicht: Risikostufen

- → KI-Systeme mit unannehmbaren Risiken sind verboten (z. B. soziale Bewertungssysteme und manipulative KI).
- → KI-Systeme mit hohem Risiko (zentrales Element) – betrifft Anbieter (Entwickler)
- → KI-Systeme mit begrenztem Risiko: geringere Transparenzpflichten: Entwickler und Betreiber müssen sicherstellen, dass Endnutzer:innen wissen, dass sie mit KI interagieren (Chatbots und Deepfakes).
- → Unreguliert: KI-Systeme mit geringstem Risiko (Vielzahl von KI-Anwendungen, die derzeit auf dem EU-Binnenmarkt erhältlich sind, z.B. Videospiele und Spam-Filter => ändert sich mit generativer KI).

Quelle: ml-ops.org

Der EU AI Act in der Übersicht: Was ist verboten (Beispiele)?

Social Scoring

- Menschen anhand ihres sozioökonomischen Status oder ihrer Persönlichkeitsmerkmale kategorisieren.

Biometrische Identifikationssysteme

- zur Massenüberwachung in öffentlichen Räumen eingesetzt, außer in Fällen schwerwiegender Bedrohungen der öffentlichen Sicherheit.

Kinder- und Jugendschutz

- gefährliches Verhalten bei Kindern fördern oder die Schwachstellen bestimmter schutzbedürftiger Gruppen ausnutzen.

Deepfakes

- Bild-, Audio- oder Videoinhalte auf hochrealistische, aber unwahre Weise generieren oder manipulieren. Hinweispflicht!

Emotionserkennung

- um die emotionalen Zustände von Menschen am Arbeitsplatz zu überwachen.

Der EU AI Act in der Übersicht: Anforderungen bei hohem Risiko

- → Einrichtung eines Risikomanagementsystems für den gesamten Lebenszyklus des KI-Systems mit hohem Risiko;
- → Durchführung von Data Governance, um sicherzustellen, dass die Schulungs-, Validierungs- und Testdatensätze relevant, ausreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sind.
- → Erstellung von technischen Unterlagen
  - zum Nachweis der Konformität und
  - Bereitstellung von Informationen für die Behörden, um die Konformität zu bewerten.
- → Bereitstellung von Gebrauchsanweisungen für nachgeschaltete Verteiler, damit diese die Vorschriften einhalten können.
- → Möglichkeit zur Implementierung einer menschlichen Aufsicht
- → Erreichung eines angemessenen Maßes an Genauigkeit, Robustheit und Cybersicherheit
- → Einrichtung eines Qualitätsmanagementsystems zur Gewährleistung der Einhaltung der Vorschriften.

Der EU AI Act in der Übersicht: Anwendungsfälle

→ Allgemeine und berufliche Bildung:
- KI-Systeme, die den Zugang, die Zulassung oder die Zuweisung zu Bildungs- und Berufsbildungseinrichtungen auf allen Ebenen bestimmen.
- Bewertung von Lernergebnissen, einschließlich derer, die zur Steuerung des Lernprozesses der Lernenden verwendet werden.
- Bewertung des angemessenen Bildungsniveaus für eine Person.
- Überwachung und Erkennung von unzulässigem Verhalten der Lernenden bei Prüfungen

→ Beschäftigung, Arbeitnehmermanagement und Zugang zur Selbständigkeit:
- KI-Systeme für die Einstellung oder Auswahl, insbesondere für gezielte Stellenanzeigen, die Analyse und Filterung von Bewerbungen und die Bewertung von Kandidat:innen.
- Beförderung und Beendigung von Verträgen, Zuweisung von Aufgaben auf der Grundlage von Persönlichkeitsmerkmalen oder Eigenschaften und Verhalten
- Überwachung und Bewertung der Leistung.

Der EU AI Act in der Übersicht: General Purpose AI (GPAI)

- → Beispiele: ChatGPT, Co-Pilot, Gemini
- → Offenlegung, dass der Inhalt durch KI generiert wurde;
- → Gestaltung des Modells, um zu verhindern, dass es illegale Inhalte erzeugt;
- → Veröffentlichung von Zusammenfassungen urheberrechtlich geschützter Daten, die für das Training verwendet wurden.
- → Anbieter von GPAI-Modellen mit freien und offenen Lizenzen müssen lediglich das Urheberrecht einhalten und die Zusammenfassung der Trainingsdaten veröffentlichen
- → Alle Anbieter von GPAI-Modellen, die ein systemisches Risiko darstellen – ob offen oder geschlossen -, müssen Modellbewertungen und Gegentests durchführen, schwerwiegende Vorfälle verfolgen und melden und Maßnahmen zur Informationssicherheit gewährleisten.

Aufgabe 1: Fallstudie

→ **Teil 1 (20 Punkte): Geschäftsprozessmodellierung**:

- Untersucht einen (hinreichend komplexen) Geschäftsprozess in einer Organisation Eurer Wahl im privaten oder im öffentlichen Sektor.
- Der Geschäftsprozess muss zumindest teilweise personenbezogene Daten im Sinne des DSGVO Art. 4 (1) verarbeiten
- Modellierung der Ablauforganisation mit BPMN.

→ **Teil 2 (10 Punkte): Datenschutz und Informationssicherheit:**

- Welche personenbezogenen Daten werden wie in eurem Prozess verarbeitet? Nennt die Rechtsgrundlage der Verarbeitung.
- Welche technischen und organisatorischen Maßnahmen (TOM) sind für die Verarbeitung vorgesehen und welchen Schutzzielen des Datenschutzes sind diese zuzuordnen? Sind keine vorgesehen, schlagt mind. 5 Maßnahmen vor, die die Sicherheit der Datenverarbeitung erhöhen würde.

→ **Teil 3 (10 Punkte): Reflexion (500 Wörter)**