thws Technische Hochschule Würzburg-Schweinfurt

FAKULTÄT INFORMATIK UND WIRTSCHAFTSINFORMATIK

VORLESUNGSSKRIPT

Datenschutzrecht I – Grundlagen & Anwendungsbereich

Geschichte, Schutzgut, Anwendungsbereich und Grundsätze der DSGVO

MODUL
Governance, Risk, Compliance & Ethics – Teil 2

SEMESTER
WS 26/27

VERSION
1.0

Prof. Dr. Markus Oermann
Dozent
markus.oermann@thws.de

Technische Hochschule Würzburg-Schweinfurt
Stand: 23.07.2026

Inhalt

In der ersten Einheit haben wir uns mit ethischen Werten wie Sicherheit, Freiheit und Selbstbestimmung beschäftigt. Das Datenschutzrecht ist nun das erste Gebiet des Rechts, das wir betrachten, welches einen dieser Werte, die informationelle Selbstbestimmung, in mit staatlicher Gewalt durchsetzbare Pflichten übersetzt. Dieses Skript legt das Fundament: Es klärt, *warum* es Datenschutz gibt, *was* er schützt, *wo* er gilt und nach welchen *Grundsätzen* jede Datenverarbeitung zu beurteilen ist. Ziel ist es, Ihnen ein belastbares Prüfraster an die Hand zu geben, mit dem Sie in der Praxis der Informationssicherheit erkennen, wann das Datenschutzrecht greift und welche Maßstäbe es anlegt.

01
KAPITEL

Mythen, Schutzgut und Geschichte

1.1 Der Mythos „Dateneigentum" und die Abgrenzung von Datenschutz und Datensicherheit

Im allgemeinen Sprachgebrauch werden Datenschutz und Datensicherheit oftmals großzügig synonym verwendet. Juristisch betrachtet handelt es sich jedoch um zwei zu unterscheidende Rechtsgebiete mit unterschiedlichen Schutzrichtungen.

Die *Datensicherheit* – oder präziser: die Informationssicherheit – zielt auf den Schutz der Hard- und Software sowie der *Daten an sich* bzw. der in ihnen repräsentierten Informationen vor Verlust, Zerstörung oder Missbrauch ab. Hier geht es primär um die Abwehr von Angreifern und technischen Störungen, also um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Der *Datenschutz* hingegen schützt die natürliche Person, die hinter den Daten steht, vor der Verletzung ihrer Persönlichkeitsrechte. Beide Felder überschneiden sich – ohne technische Datensicherheit ist Datenschutz nicht umsetzbar –, aber sie verfolgen unterschiedliche Zwecke.

Wichtig ist eine weitere Klarstellung: Es geht im europäischen Datenschutz nicht um die ««Frage, „wem die Daten gehören". Ein Konzept des rechtlichen „Dateneigentums" existiert in Deutschland und der EU schlichtweg nicht. Vielmehr will der Datenschutz die Bürgerinnen und Bürger präventiv in Situationen struktureller Machtasymmetrien beim Umgang mit personenbezogenen Daten schützen. Sei es gegenüber dem Staat oder gegenüber mächtigen Wirtschaftsunternehmen. Schließlich weiß der Datenverarbeiter grundsätzlich viel besser als wir selbst, welche Informationen über uns gespeichert sind und wie sie verarbeitet werden. Diese Ungleichverteilung von Wissen und Macht versucht der Datenschutz abzumildern.

DEFINITION

Datensicherheit vs. Datenschutz

Datensicherheit schützt die *Daten* vor Verlust und Missbrauch; Datenschutz schützt die *Person* hinter den Daten vor Persönlichkeitsrechtsverletzungen.

1.2 Das Volkszählungsurteil und das Recht auf informationelle Selbstbestimmung

Das deutsche Datenschutzrecht fußt maßgeblich auf einer historischen Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1983, dem sogenannten Volkszählungsurteil. Hintergrund war eine geplante Volkszählung, gegen die sich eine breite gesellschaftliche Protestbewegung formierte: Tausende Menschen fürchteten die umfassende statistische Erfassung und sahen darin den Beginn eines überwachenden Staates. Das Gericht leitete in seiner Entscheidung aus der Menschenwürde (Art. 1 Abs. 1 GG) in Verbindung mit dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) das Grundrecht auf *informationelle Selbstbestimmung* ab.

Die Kernidee dieses Grundrechts lautet: Jeder Mensch darf grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen – er darf also selbst entscheiden, wem er welche persönlichen Lebenssachverhalte offenbart. Das Gericht stellte zugleich klar, dass es unter den Bedingungen der automatisierten Datenverarbeitung kein „belangloses Datum" mehr gibt: Auch eine für sich genommen unscheinbare Information kann durch Verknüpfung mit anderen Daten erhebliche Bedeutung für das Persönlichkeitsbild gewinnen.

DEFINITION

Informationelle Selbstbestimmung

Das aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG abgeleitete Grundrecht, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen.

1.3 Panopticon und Chilling Effect: warum der Schutz ein kollektives Anliegen ist

Warum aber ist die Erfassung von Daten überhaupt ein Problem, wenn man „nichts zu verbergen" hat? Die Antwort liefert ein Bild aus der politischen Philosophie: das **Panopticon**, ein von Jeremy Bentham, dem Mitbegründer der Utilitarismus, entworfenes Gefängnis, in dem ein einzelner Wächter im Zentrum alle Insassen jederzeit beobachten könnte, ohne dass diese wissen, ob sie gerade beobachtet werden. Die bloße *Möglichkeit* der Beobachtung diszipliniert das Verhalten. Der französische Sozialphilosoph Michel Foucault machte später dieses Modell zur Metapher moderner Überwachungsgesellschaften. In seinem Werk „Überwachen und Strafen" beschreibt er, wie eine Gesellschaft der totalen Sichtbarkeit zu einer totalen Kontrolle und damit zur Unterdrückung von Individualität und Widerstand führt.

Genau hier setzt das Volkszählungsurteil an. Es schützt vor dem sogenannten **Chilling Effect** (Abschreckungseffekt): Wer fürchten muss, dass abweichende Verhaltensweisen jederzeit notiert und informationstechnisch verarbeitet werden, passt sein Verhalten unweigerlich an den vermeintlichen Mainstream an. Das Gericht formulierte, mit einer Gesellschaftsordnung, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß, sei das Recht auf informationelle Selbstbestimmung nicht vereinbar. Damit bemüht das Gericht zwei Argumente: ein **individuelles** (Schutz der Persönlichkeitsentfaltung) und ein **kollektives** (Selbstbestimmung als Funktionsvoraussetzung einer freiheitlichen, demokratischen Gemeinwesens).

Datenschutz ist deshalb nicht bloß individueller Geheimnisschutz, sondern schützt Grundlagen der Demokratie.

ÜBUNG · BEGRIFFE

Das gedachte Gefängnis, in dem die bloße **Möglichkeit** der Beobachtung das Verhalten diszipliniert, heißt **Panopticon**. Die daraus folgende Abschreckung von der Grundrechtsausübung nennt man in der verfassungsrechtlichen Debatte **Chilling Effect**.

1.4 Vom Recht auf informationelle Selbstbestimmung zum IT-Grundrecht und zur DSGVO

Das Verfassungsrecht blieb nicht beim Volkszählungsurteil stehen. Im Jahr 2008 entwickelte das Bundesverfassungsgericht in der Entscheidung zur sogenannten Online-Durchsuchung ein weiteres, neues Grundrecht: das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** – kurz das **IT-Grundrecht** oder „Computer-Grundrecht". Es schützt nicht einzelne Daten, sondern das informationstechnische System (Laptop, Smartphone) als Ganzes vor heimlichem staatlichem Zugriff, weil solche Systeme heute einen umfassenden Einblick in die Persönlichkeit erlauben. Damit reagiert das Verfassungsrecht auf eine Welt, in der nicht mehr einzelne Akten oder Dateien, sondern vernetzte Geräte das eigentliche Schutzobjekt sind.

Auf einfachgesetzlicher Ebene durchlief der Datenschutz eine lange Entwicklung: vom weltweit ersten Datenschutzgesetz des Landes Hessen (1970) über das erste Bundesdatenschutzgesetz (1977) und die europäische Datenschutzrichtlinie (1995) bis hin zur **Datenschutz-Grundverordnung (DSGVO)**, die 2016 in Kraft trat und seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedstaaten gilt. Die DSGVO löste den Flickenteppich nationaler Umsetzungsgesetze ab und schuf ein weitgehend einheitliches, unmittelbar geltendes Datenschutzrecht mit empfindlichen Sanktionsmöglichkeiten – ein Modell, das weltweit als Vorbild wirkt.

QUICK-CHECK

Welches Grundrecht entwickelte das Bundesverfassungsgericht im Volkszählungsurteil (1983)?

- Das IT-Grundrecht (Vertraulichkeit und Integrität informationstechnischer Systeme)
- **Das Recht auf informationelle Selbstbestimmung**
- Das Recht auf Dateneigentum
- Das Fernmeldegeheimnis

1.5 Datenschutz im Mehrebenen-System

Die rechtlichen Vorgaben für den Datenschutz finden sich in Gesetzen, Verordnungen und nicht zuletzt in der Judikatur der Gerichte sowie in Hinweisen der Aufsichtsbehörden auf verschiedenen Ebenen.

Auf Ebene der Europäischen Union entfaltet die DSGVO als Verordnung unmittelbare Geltung in allen Mitgliedstaaten. Sie greift für automatisierte sowie für nicht-automatisierte Datenverarbei-

tungen, sofern letztere in einem strukturierten Dateisystem durchgeführt werden. Auf nationaler Ebene wird die DSGVO durch das Bundesdatenschutzgesetz (BDSG) sowie durch Spezialgesetze wie das Telekommunikations-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ergänzt; die DSGVO enthält dafür sogenannte Öffnungsklauseln, die den Mitgliedstaaten Regelungsspielräume belassen. Für Akteure auf Länderebene, wie beispielsweise Hochschulen, gelten zusätzlich die jeweiligen Landesdatenschutzgesetze. Hinzu treten die Auslegung durch den Europäischen Gerichtshof, Leitlinien des Europäischen Datenschutzausschusses (EDSA) und die Praxis der nationalen Aufsichtsbehörden.

02
KAPITEL

Anwendbarkeit der DSGVO

2.1 Sachliche und räumliche Anwendbarkeit in der Praxis

Damit das scharfe Schwert der DSGVO überhaupt gezogen werden kann, müssen fundamentale Einstiegsvoraussetzungen erfüllt sein.

Die **sachliche** Anwendbarkeit fordert nach Art. 2 DSGVO eine ganz oder teilweise automatisierte Verarbeitung von personenbezogenen Daten. Alternativ genügt es, wenn die Daten nicht-automatisiert in einem strukturierten Dateisystem gespeichert werden oder gespeichert werden sollen. Ausgenommen ist insbesondere die Verarbeitung durch eine natürliche Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Dass diese Ausnahme nach Art. 2 Abs. 2 lit. c DSGVO als **Haushaltsprivileg** bezeichnet wird, ist nicht gerade glücklich. Denn nur rein private und nicht alle haushaltsbezogenen automatisieren Datenverarbeitungen sind freigestellt.

Die **räumliche** Anwendbarkeit richtet sich nach dem Niederlassungs- und dem Marktortprinzip gemäß Art. 3 DSGVO. Die Verordnung ist zwingend anzuwenden, sobald ein Verantwortlicher oder Auftragsverarbeiter eine Niederlassung innerhalb der EU unterhält und die Verarbeitung im Rahmen ihrer Tätigkeit erfolgt (Niederlassungsprinzip). Ebenso greift sie aber auch schon, wenn einer in der EU befindlichen Person Waren oder Dienstleistungen angeboten werden oder ihr Verhalten beobachtet wird (**Marktortprinzip**). Es ist juristisch damit völlig unerheblich, auf welchem Server im Silicon Valley oder anderswo auf der Welt die Daten physisch gespeichert sind.

Lassen Sie uns die Anwendbarkeitsprüfung in einer Abfolge von Prüffragen rekapitulieren:

FALLSTUDIE

Fall Anna: Instagram-Stalking in der Vorlesung

Die Studentin Anna wirft einen flüchtigen Blick auf den ungesperrten Laptop ihres Sitznachbarn. Dabei merkt sie sich seinen Instagram-Namen sowie seine Handynummer. Ihre

Absicht ist es, ihn später privat auf einen Kaffee einzuladen. Fällt dieser alltägliche Vorgang in den Anwendungsbereich der DSGVO?
Lösung. Zwar verarbeitet Anna unzweifelhaft personenbezogene Daten (Name, Nummer), jedoch geschieht dies weder automatisiert, noch speichert sie die Daten in einem strukturierten Dateisystem (Art. 2 Abs. 1 DSGVO). Selbst wenn man – mit viel juristischer Fantasie – eine DSGVO-relevante Verarbeitung annehmen würde, griffe das sogenannte „Haushaltsprivileg" nach Art. 2 Abs. 2 lit. c DSGVO. Anna verarbeitet die Daten ausschließlich für eine rein persönliche, familiäre Tätigkeit. Die DSGVO ist somit nicht anwendbar.

2.2 Personenbezogene Daten und der Begriff der Verarbeitung

Das Kernkriterium jedes Datenschutzfalls ist das Vorliegen personenbezogener Daten. Nach Art. 4 Nr. 1 DSGVO sind dies alle Informationen, die sich auf eine identifizierte oder, was weitaus häufiger vorkommt, identifizierbare lebende natürliche Person beziehen.

Dies umfasst klassische identifziertende Parameter wie Namen, Adressen und Kontonummern, erstreckt sich aber auch auf Fotos von erkennbaren Personen, Standortdaten und sogar dynamische IP-Adressen, sofern die Nutzer über realistisch verfügbare Mittel identifiziert werden können. Wichtig ist die Erkenntnis, dass das europäische Datenschutzrecht – wie schon das Volkszählungsurteil – kein „belangloses Datum" kennt. Auch scheinbar unscheinbare Datenschnipsel können durch intelligente Verknüpfung eine immense Relevanz für das Persönlichkeitsprofil entfalten. Echte synthetische Daten, rein maschinengenerierte Werte (etwa der Stromverbrauch einer Fräse) oder Daten von Verstorbenen fallen hingegen mangels einer lebenden natürlichen Person aus dem Schutzbereich heraus.

ÜBUNG · BEGRIFFE

Die Verarbeitung von Daten, die ohne Weiteres beim Betrieb einer Maschine anfallen, fällt **nicht** unter die DSGVO, da es sich nicht um **personenbezogene** Daten handelt. Eine IP-Adresse ist jedoch geschützt, sofern der Nutzer **identifizierbar** ist.

Testen Sie im folgenden interaktiven Szenario-Checker selbst, welche Datenarten als personenbezogen klassifiziert werden.

Der **Begriff der Verarbeitung** im Sinne von Art. 4 Nr. 2 DSGVO ist denkbar weit gefasst. Er erfasst praktisch jeden Umgang mit Daten: vom Erheben und Speichern über das Verändern und Übermitteln bis hin zum Löschen. Ein juristischer Grenzfall ist beispielsweise das Anbringen analoger, nicht alphabetisch sortierter Klingelschilder an einem Mehrfamilienhaus. Dies stellt in der Regel keine Verarbeitung im Sinne der DSGVO dar, da der Vorgang weder automatisiert abläuft noch Teil eines strukturierten Dateisystems ist.

2.3 Verantwortlicher und Auftragsverarbeiter

Wer die DSGVO einhalten muss, ist keine triviale Vorfrage – sie entscheidet darüber, an wen sich Pflichten und Bußgelder richten. Die Verordnung unterscheidet zwei zentrale Rollen.

Der **Verantwortliche** ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die *Zwecke und Mittel* der Verarbeitung entscheidet. Vereinfacht: Wer das „Warum" und das „Wie" der Datenverarbeitung bestimmt, ist verantwortlich und trägt die Hauptlast der datenschutzrechtlichen Pflichten.

Der **Auftragsverarbeiter** hingegen ist nach Art. 4 Nr. 8 DSGVO eine Stelle, die personenbezogene Daten *im Auftrag* des Verantwortlichen verarbeitet, ohne selbst über Zwecke und Mittel zu entscheiden. Das klassische Beispiel ist ein Cloud-Hosting-Anbieter oder ein externer Lohnabrechnungsdienst.

Diese Rollenverteilung wird vertraglich abgesichert. Für die Auftragsverarbeitung verlangt Art. 28 DSGVO einen **Auftragsverarbeitungsvertrag (AVV)**, der unter anderem Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie die Weisungsbindung des Auftragsverarbeiters festlegt.

Treffen mehrere Stellen *gemeinsam* die Entscheidung über Zwecke und Mittel, liegt eine **gemeinsame Verantwortlichkeit** (Art. 26 DSGVO) vor; die Beteiligten müssen dann in einer Vereinbarung transparent festlegen, wer welche Pflichten – insbesondere gegenüber den betroffenen Personen – erfüllt.

Die korrekte Bestimmung der Rolle ist in der Praxis hochrelevant: Sie entscheidet darüber, wer haftet, wer Informationspflichten erfüllen muss und gegen wen sich Betroffenenrechte richten.

DEFINITION

Verantwortlicher vs. Auftragsverarbeiter

Der Verantwortliche entscheidet über *Zwecke und Mittel* der Verarbeitung (Art. 4 Nr. 7); der Auftragsverarbeiter verarbeitet die Daten weisungsgebunden *im Auftrag* (Art. 4 Nr. 8), abgesichert durch einen Vertrag nach Art. 28.

QUICK-CHECK

Ein Online-Shop nutzt einen externen Cloud-Anbieter, um seine Kundendatenbank zu hosten. Der Anbieter speichert die Daten nur nach Weisung des Shops. Welche Rolle hat der Cloud-Anbieter?

Verantwortlicher
Auftragsverarbeiter
Gemeinsam Verantwortlicher
Betroffene Person

03

KAPITEL

Die Grundsätze der Datenverarbeitung

Ist die DSGVO anwendbar, so muss jede einzelne Verarbeitungsaktivität den strengen Vorgaben des Art. 5 DSGVO genügen. Diese Prinzipien bilden das normative Fundament des Datenschutzes – sie sind der Maßstab, an dem sich jede Verarbeitung messen lassen muss, und sie werden in den folgenden Einheiten durch konkrete Pflichten und Rechte ausbuchstabiert.

Das wichtigste Prinzip ist das der **Rechtmäßigkeit**. Es besagt, dass eine Verarbeitung personenbezogener Daten im Sinne der DSGVO zunächst einmal verboten ist, es sei denn, es liegt eine Einwilligung oder eine andere Erlaubnisnorm vor. Dies weicht vom sonstigen Default unserer liberalen Rechtsordnung, in der erstmal alles erlaubt ist, was nicht anders geregelt ist, für den Bereich des Datenschutzes ab.

Die Prinzipien der Verarbeitung nach **Treu und Glauben** sowie der **Transparenz** gebieten, dass die Betroffenen nachvollziehen können, was mit ihren Daten geschieht. Betroffene dürfen zudem nicht durch irreführende Praktiken oder Dark Patterns ausgetrickst werden.

Die streng zu beachtende **Zweckbindung** gebietet, dass für jede Datenverarbeitung ein festgelegter, eindeutiger und legitimer Zweck vorliegen muss, und verhindert, dass Daten für unvereinbare, völlig neue Zwecke zweckentfremdet werden.

Das Prinzip der **Datenminimierung** fordert den Verzicht auf überflüssige Datensammlungen: Es dürfen nur so viele Daten erhoben werden, wie zur Zweckerreichung notwendig sind. Flankiert wird dies durch die **Speicherbegrenzung**, die eine Löschung anordnet, sobald der Zweck entfällt.

Schließlich müssen die Daten sachlich **richtig** sein und durch geeignete technische und organisatorische Maßnahmen vor unbefugtem Zugriff geschützt werden (**Integrität und Vertraulichkeit**).

Dies alles umspannt die **Rechenschaftspflicht** (Accountability): Die Nachweislast für die Einhaltung all dieser Pflichten trägt stets der Verantwortliche. Er muss die Konformität nicht nur herstellen, sondern auch dokumentieren und belegen können. Auch hier weicht das Datenschutzrecht vom üblichen Default in unserer Rechtsordnung ab, wonach Nachweispflichten in der Regel bei den Trägern öffentlicher Gewalt liegen.

Erkunden Sie die verschiedenen Grundsätze interaktiv, um deren spezifische Bedeutung im Kontext der DSGVO zu vertiefen.

QUICK-CHECK

Welcher Grundsatz besagt, dass Daten gelöscht werden müssen, sobald sie für den ursprünglichen Erhebungszweck nicht mehr benötigt werden?

Datenminimierung
Speicherbegrenzung
Zweckbindung
Integrität und Vertraulichkeit

DEEP DIVE Vertiefung: Rechenschaftspflicht als Paradigmenwechsel

Die in Art. 5 Abs. 2 DSGVO verankerte Rechenschaftspflicht markiert einen Wechsel der Beweislast. Während früher die Aufsichtsbehörde einen Verstoß nachweisen musste, muss heute der Verantwortliche aktiv belegen, dass er die Grundsätze einhält – durch Verzeichnisse von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzungen und dokumentierte technische und organisatorische Maßnahmen. Diese Pflicht ist das Scharnier zwischen den abstrakten Grundsätzen dieser Einheit und den konkreten Compliance- und Dokumentationspflichten, die in den späteren Einheiten behandelt werden.

Damit ist das Fundament des Datenschutzrechts gelegt: Wir wissen nun, *warum* es Datenschutz gibt, *was* er als Schutzgut der informationellen Selbstbestimmung bewahrt, *wann* die DSGVO anwendbar ist und nach welchen *Grundsätzen* jede Verarbeitung zu beurteilen ist. Die nächste Einheit wird zeigen, auf welche konkreten Rechtsgrundlagen eine Verarbeitung gestützt werden kann, welche Pflichten den Verantwortlichen treffen und welche Rechte die betroffenen Personen ihm entgegensetzen können.

04
KAPITEL

Quellen

4.1 Normen & Standards

- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), insb. Art. 2, Art. 3, Art. 4 Nr. 1, 2, 7, 8, Art. 5, Art. 26, Art. 28. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679
- Bundesdatenschutzgesetz (BDSG) in der Fassung vom 30.06.2017. https://www.gesetze-im-internet.de/bdsg_2018/
- Grundgesetz für die Bundesrepublik Deutschland, Art. 1 Abs. 1, Art. 2 Abs. 1. https://www.gesetze-im-internet.de/gg/

4.2 Rechtsprechung

- BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u. a. (Volkszählung), BVerfGE 65, 1.
- BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 (Online-Durchsuchung / IT-Grundrecht), BVerfGE 120, 274.