thws Technische Hochschule Würzburg-Schweinfurt

FAKULTÄT INFORMATIK UND WIRTSCHAFTSINFORMATIK

VORLESUNGSSKRIPT

Datenschutzrecht

Einführung und Grundfragen

MODUL
ELSI und Digitalisierung

SEMESTER
SoSe 26

VERSION
1.0

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

Technische Hochschule Würzburg-Schweinfurt
Stand: 21.04.2026

Inhalt

1 Einführung – Mythen, Geschichte und Rechtsquellen 3
1.1 Der Mythos „Dateneigentum“ und der Irrtum über das Verhältnis von Datenschutz und Datensicherheit 3
1.2 Historischer Ursprung: Das Volkszählungsurteil 3
1.3 Datenschutz im Mehrebenen-System 4
2 Grund- und Abgrenzungsfragen 5
2.1 Räumliche und Sachliche Anwendbarkeit in der Praxis 5
2.2 Personenbezogene Daten und der Begriff der Verarbeitung 5
2.3 Die goldenen Grundsätze der Datenverarbeitung 6

Dieses Skript ist für Ihr Selbststudium konzipiert. Ergänzt wird die theoretische Fundierung durch einschlägige Fallbeispiele aus der juristischen Praxis.

01
KAPITEL

Einführung – Mythen, Geschichte und Rechtsquellen

1.1 Der Mythos „Dateneigentum“ und der Irrtum über das Verhältnis von Datenschutz und Datensicherheit

Im allgemeinen Sprachgebrauch werden Datenschutz und Datensicherheit oftmals recht 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* vor Verlust, Zerstörung oder Missbrauch ab. Hier geht es primär um die Abwehr von Hackern und technischen Störungen. Der *Datenschutz* hingegen schützt die natürliche Person, die hinter den Daten steht, vor der Verletzung ihrer Persönlichkeitsrechte.

Wichtig ist dabei eine Klarstellung: Es geht im europäischen Datenschutz nicht um die zivilrechtliche 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 grundsätzlichviel 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 Historischer Ursprung: Das Volkszählungsurteil

Das deutsche Datenschutzrecht fußt maßgeblich auf einer historischen Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1983, dem sogenannten Volkszählungsurteil. Das Gericht

leitete damals aus der Menschenwürde (Art. 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 entscheiden, wem er welche persönlichen Lebenssachverhalte offenbart.

Dieses Recht schützt uns vor dem sogenannten Panopticon-Effekt. Wer fürchten muss, dass abweichende Verhaltensweisen jederzeit notiert und informationstechnisch verarbeitet werden, passt sein Verhalten unweigerlich an den vermeintlichen Mainstream an. Dies bedroht die individuelle Selbstbestimmung und gefährdet in letzter Konsequenz die liberale Grundordnung unserer Gesellschaft. Beide Arguemnte - das indivdiuelle und das kollektive - bemüht auch das Bundesverfassungsgericht.

1.3 Datenschutz im Mehrebenen-System

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

Auf Ebene der Europäischen Union entfaltet die Datenschutz-Grundverordnung (DSGVO) als Verordnung unmittelbare Geltung in allen Mitgliedstaaten. Sie greift für automatisierte sowie für nicht-automatisierte Datenverarbeitungen, sofern letztere in einer strukturierten Dateisystem gespeichert sind. Auf nationaler Ebene wird die DSGVO durch das Bundesdatenschutzgesetz (BDSG) sowie durch Spezialgesetze wie das TDDDG für Telemedien ergänzt. Für Akteure auf Länderebene, wie beispielsweise Hochschulen, gelten zusätzlich die jeweiligen Landesdatenschutzgesetze.

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.

02
KAPITEL

Grund- und Abgrenzungsfragen

2.1 Räumliche und Sachliche Anwendbarkeit in der Praxis

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

Die räumliche Anwendbarkeit richtet sich nach dem Niederlassungs- und dem Marktortprinzip gem. Art. 3 DSGVO. Die Verordnung ist zwingend anzuwenden, sobald ein Unternehmen eine Niederlassung innerhalb der EU unterhält. Ebenso greift sie, wenn Daten von in der EU ansässigen Personen mit Bezug auf den europäischen Markt verarbeitet werden (Marktortprinzip). Es ist juristisch völlig unerheblich, auf welchem Server im Silicon Valley oder anderswo auf der Welt die Daten physisch gespeichert sind.

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.

Lassen Sie uns die Anwendbarkeitsprüfung an einem strukturierten Prozessdurchlauf exemplarisch untersuchen.

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 Parameter wie Namen, Adressen und Kontonummern, erstreckt sich aber auch auf Fotos, Standortdaten und sogar dynamische IP-Adressen, sofern die Nutzer über Auskunftsansprüche identifiziert werden können. Wichtig ist die Erkenntnis, dass das europäische Datenschutzrecht 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. Bei Ultraschallbildern eines Fötus wird juristisch vortrefflich gestritten: Der Fötus selbst ist noch keine rechtsfähige natürliche Person, sehr wohl aber können die visualisierten Gesundheitsdaten der werdenden Mutter zugerechnet werden.

ÜBUNG · BEGRIFFE

Die Verarbeitung von Daten aus einer reinen Maschine 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 Wohnhaus. Dies stellt in der Regel keine Verarbeitung dar, da der Prozess weder automatisiert abläuft noch Teil eines strukturierten Dateisystems ist.

2.3 Die goldenen Grundsätze der Datenverarbeitung

Ist die DSGVO anwendbar, so muss jede einzelne Verarbeitungsaktivität den strengen Vorgaben des Art. 5 DSGVO genügen. Diese „Goldenen Grundsätze“ bilden das normative Fundament des Datenschutzes.

Die Prinzipien der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben sowie der Transparenz gebieten, dass für jede Handlung eine Erlaubnisnorm vorliegen muss und 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 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 absolut 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 Maßnahmen vor unbefugtem Zugriff geschützt werden (Integrität und Vertraulichkeit). Die Nachweislast für die Einhaltung all dieser Pflichten trägt stets der Verantwortliche (Rechenschaftspflicht).

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