thws Technische Hochschule Würzburg-Schweinfurt

FAKULTÄT INFORMATIK UND WIRTSCHAFTSINFORMATIK

VORLESUNGSSKRIPT

Datenschutzrecht III – Datensicherheit, Compliance & Durchsetzung

Technische und organisatorische Pflichten, das Sanktionsregime und seine Durchsetzung

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

1 Verantwortung und Nachweis: die Dokumentationspflichten ... 3
1.1 Rechenschaft und Verantwortung (Art. 24 DSGVO) ... 3
1.2 Das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) ... 4
1.3 Die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) ... 4
2 Datensicherheit: technische und organisatorische Maßnahmen ... 5
2.1 Der „Stand der Technik" ... 6
2.2 Privacy by Design und Privacy by Default (Art. 25 DSGVO) ... 6
3 Wenn der Schutz versagt: Meldepflichten bei Datenpannen ... 7
4 Die regulierte Selbstkontrolle: der Datenschutzbeauftragte ... 8
5 Durchsetzung von außen: Aufsichtsbehörden, Bußgelder und Haftung ... 9
5.1 Der „One-Stop-Shop" und das Forum Shopping ... 9
5.2 Die Geldbußen (Art. 83 DSGVO) ... 9
5.3 Der Schadensersatzanspruch (Art. 82 DSGVO) ... 10
5.4 Straftatbestände: § 42 BDSG und §§ 201 ff. StGB ... 10
6 Einzelfrage: Videoüberwachung ... 11
7 Ausblick: von der Datensicherheit zum Informationssicherheitsrecht ... 13
8 Quellen ... 13
8.1 Normen & Standards ... 13
8.2 Rechtsprechung ... 14

In der vorangegangenen Einheit haben wir gesehen, *unter welchen Voraussetzungen* eine Verarbeitung personenbezogener Daten rechtmäßig ist: Wir haben die Rechtsgrundlagen des Art. 6 DSGVO, die Anforderungen an eine wirksame Einwilligung, den verschärften Schutz besonderer Datenkategorien (Art. 9) sowie die Informationspflichten und die Betroffenenrechte (Art. 12–21) durchgearbeitet. Das alles bleibt jedoch weitgehend ohne Wirkung, solange es nicht durch robuste Technik und Organisation flankiert und vor allem schlagkräftig durchgesetzt wird. Das Datenschutzrecht bliebe ein zahnloser Tiger, wenn die Verarbeitung zwar formal erlaubt, aber technisch ungeschützt und faktisch unkontrolliert abliefe.

Diese Einheit schließt damit den Datenschutz-Block ab. Sie behandelt drei zusammenhängende Fragen: Wie muss der Verantwortliche seine Verarbeitung *dokumentieren* und vorab auf Risiken *prüfen*? Wie muss er seine Systeme *organisatorisch rahmenn und technisch absichern*? Und was geschieht, wenn er all dies versäumt – also wie wird die DSGVO *durchgesetzt und sanktioniert*? Den roten Faden bildet die Erkenntnis, dass die DSGVO dem Verantwortlichen die **Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO) auferlegt: Er muss die Einhaltung aller Grundsätze nicht nur gewährleisten, sondern auch nachweisen können.

01
KAPITEL

Verantwortung und Nachweis: die Dokumentationspflichten

In der betrieblichen Praxis konvergieren die Welten der IT-Sicherheit und der Datenschutz-Compliance, auch wenn sie juristisch zu trennen sind. Die **Datensicherheit** (oder auch Informationssicherheit) zielt institutionell auf den Schutz von Hardware, Software und Datenbeständen gegen Verlust, Zerstörung oder Missbrauch durch Unbefugte. Es geht darum, Informationsverluste zu vermeiden. Der **Datenschutz** hingegen stellt die natürliche Person ins Zentrum und schützt sie vor Persönlichkeitsrechtsverletzungen. Diese begriffliche Trennung ist wichtig, weil sie erklärt, warum dieselbe Maßnahme, etwa eine Verschlüsselung, aus zwei Blickwinkeln gefordert sein kann.

1.1 Rechenschaft und Verantwortung (Art. 24 DSGVO)

Den Ausgangspunkt aller organisatorischen und technischen Pflichten bildet Art. 24 DSGVO. Er verpflichtet den Verantwortlichen, *geeignete technische und organisatorische Maßnahmen* umzusetzen, um sicherzustellen *und den Nachweis erbringen zu können*, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. Art. 24 ist damit die organisatorische Konkretisierung der Rechenschaftspflicht aus Art. 5 Abs. 2: Es genügt nicht, rechtmäßig zu handeln. Man muss dies belegen können. Aus dieser Beweislastumkehr folgen die konkreten Dokumentationsinstrumente.

1.2 Das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Das operationelle Herzstück der Compliance ist das **Verzeichnis von Verarbeitungstätigkeiten (VVT)**. Art. 30 DSGVO verlangt die lückenlose Dokumentation aller Datenverarbeitungsprozesse einer Organisation. Das Verzeichnis dient als Nachweis gegenüber den Aufsichtsbehörden, dass die Verarbeitung rechtmäßig und kontrolliert erfolgt. Es muss unter anderem den Namen und die Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung, eine Beschreibung der Kategorien betroffener Personen und personenbezogener Daten, die Empfängerkategorien, etwaige Drittlandübermittlungen, die vorgesehenen Löschfristen sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen enthalten.

Eine vielzitierte, in der Praxis aber trügerische Erleichterung enthält Art. 30 Abs. 5 DSGVO: Unternehmen mit weniger als 250 Beschäftigten sind von der Verzeichnispflicht grundsätzlich befreit. Diese Ausnahme greift jedoch *nicht*, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der Betroffenen birgt, nicht nur gelegentlich erfolgt oder besondere Datenkategorien (Art. 9) bzw. strafrechtsbezogene Daten betrifft. Da praktisch jedes Unternehmen mit Beschäftigten regelmäßig deren Daten verarbeitet, läuft die vermeintliche Befreiung für den Normalfall leer.

DEFINITION

Verzeichnis von Verarbeitungstätigkeiten (VVT)

Die nach Art. 30 DSGVO verpflichtende, systematische Bestandsaufnahme *aller* Verarbeitungsprozesse einer Organisation. Das ist das zentrale Nachweisinstrument der Rechenschaftspflicht gegenüber der Aufsichtsbehörde.

1.3 Die Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Während das VVT *jede* Verarbeitung erfasst, greift die **Datenschutz-Folgenabschätzung (DSFA)** nur bei besonders riskanten Vorhaben. Art. 35 DSGVO verlangt eine strukturierte Vorab-Risikobewertung immer dann, wenn eine Form der Verarbeitung voraussichtlich ein *hohes Risiko* für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Das ist insbesondere bei Einsatz neuer Technologien der Fall. Was als „hohes Risiko“ zu werten ist, bestimmt sich nicht starr, sondern ergibt sich aus der kumulativen Betrachtung verschiedener Kriterien: Intensität und Umfang, Dauer der Verarbeitung, Art der verarbeiteten Daten, Konsequenzen und mögliche Folgen für Betroffene sowie die Wahrscheinlichkeit des Eintritts. Das Gesetz nennt drei Regelbeispiele: die systematische und umfassende Bewertung persönlicher Aspekte (Profiling/Scoring), die umfangreiche Verarbeitung besonderer Datenkategorien und die systematische weiträumige Überwachung öffentlich zugänglicher Bereiche.

Die DSFA ist ein vorgelagertes Verfahren der Risikofolgenabschätzung: Der Verantwortliche muss die geplanten Verarbeitungsvorgänge beschreiben, ihre Notwendigkeit und Verhältnismäßigkeit bewerten, die Risiken für die Betroffenen abschätzen und die zur Risikobewältigung geplanten Abhilfemaßnahmen darlegen. Lässt sich ein hohes Risiko durch die Maßnahmen nicht eindämmen, muss der Verantwortliche vor Beginn der Verarbeitung die Aufsichtsbehörde konsultieren (Art. 36). Die DSFA ist damit das zentrale Scharnier zwischen abstrakter Risikobewertung und

konkreter technischer Schutzmaßnahme und ein Vorgriff auf die risikobasierten Pflichten, die uns bei der KI-Verordnung erneut begegnen werden.

QUICK-CHECK

Ein Unternehmen plant ein KI-System, das die Kreditwürdigkeit von Kundinnen und Kunden automatisiert bewertet (Scoring). Welche Pflicht ist hier vorrangig zu prüfen?

Eine Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO
Eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, da ein hohes Risiko durch systematische Bewertung persönlicher Aspekte vorliegt
Die Bestellung eines Vertreters nach Art. 27 DSGVO
Keine, solange eine Einwilligung vorliegt

02
KAPITEL

Datensicherheit: technische und organisatorische Maßnahmen

Die zentrale Schnittmenge von IT-Sicherheit und Datenschutz bildet Art. 32 DSGVO zur *Sicherheit der Verarbeitung*. Verantwortliche und Auftragsverarbeiter müssen geeignete technische und organisatorische Maßnahmen („TOMs“) implementieren, um ein dem Risiko der konkreten Verarbeitung angemessenes Schutzniveau zu gewährleisten. Art. 32 nennt dafür beispielhaft die Pseudonymisierung und Verschlüsselung, die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherzustellen, die rasche Wiederherstellbarkeit nach einem Zwischenfall sowie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit dieser Maßnahmen. „TOMs” bündeln dabei zwei Ebenen: *technische* Maßnahmen wirken am System selbst (etwa Verschlüsselung), *organisatorische* Maßnahmen regeln das Verhalten der Beteiligten (etwa ein Berechtigungskonzept, das den Zugriff auf das Nötige beschränkt).

DEFINITION

Pseudonymisierung vs. Anonymisierung

Bei der Pseudonymisierung wird der Personenbezug nur *verdeckt* und lässt sich mit einem separat verwahrten Schlüssel wieder herstellen. Die Daten bleiben deshalb personenbezogen. Bei der Anonymisierung wird der Bezug *endgültig* und irreversibel entfernt, sodass die DSGVO nicht mehr greift.

2.1 Der „Stand der Technik”

Maßgeblich für die Beurteilung der Sicherheitsmaßnahmen ist der **„Stand der Technik”**. Dieser unbestimmte Rechtsbegriff meint den Entwicklungsstand fortschrittlicher Verfahren, die sich in der Praxis bereits *bewährt* haben. Er liegt bewusst zwischen zwei anderen Stufen: oberhalb des bloßen „Standes der allgemeinen anerkannten Regeln der Technik” (etablierte, möglicherweise veraltete Praxis) und unterhalb des „Standes von Wissenschaft und Forschung” (noch unerprobte Spitzentechnik). Wäre Letzteres gefordert, müssten Verantwortliche deutlich mehr leisten, als nur etablierte Industriestandards umzusetzen. Der „Stand der Technik” ist dynamisch: Was heute genügt, kann morgen unzureichend sein. So veralten spezifische Verschlüsselungsverfahren etwa.

DEEP DIVE Das Standard-Datenschutzmodell (SDM)

Zur konzeptionellen Umsetzung der TOMs dient in der behördlichen Praxis häufig das **Standard-Datenschutzmodell (SDM)**, das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder entwickelt wurde. Es übersetzt die rechtlichen Anforderungen in sieben übergeordnete **Gewährleistungsziele**: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit. So garantiert *Integrität* beispielsweise die Vollständigkeit und unverfälschte Richtigkeit der Verarbeitung, während *Nichtverkettung* technisch verhindert, dass Daten, die für unterschiedliche Zwecke erhoben wurden, unzulässig zusammengeführt werden. *Intervenierbarkeit* sorgt dafür, dass die Betroffenenrechte aus der letzten Einheit technisch überhaupt umsetzbar sind. Das SDM spezifiziert diese Ziele weiter in konkrete Anforderungen an Systemarchitektur und Prozesse. Die jeweils aktuelle Fassung findet sich auf den Seiten des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern.

Erkunden Sie im folgenden Widget, mit welchen konkreten technischen und organisatorischen Maßnahmen die abstrakten Gewährleistungsziele des SDM in der Praxis umgesetzt werden:

2.2 Privacy by Design und Privacy by Default (Art. 25 DSGVO)

Ein zentraler Innovationsansatz der DSGVO bindet Softwareentwicklung und Systemarchitektur unmittelbar an rechtliche Maßstäbe: Art. 25 DSGVO. Während Art. 32 die laufende Sicherheit adressiert, verschiebt Art. 25 den Schutz nach vorne in die Konzeptions- und Voreinstellungsphase. Hier schließt sich übrigens der Bogen zur ethischen Einheit (Kapitel 1): Das Gebot, ethische und rechtliche Anforderungen *von Anfang an* einzubauen (Collingridge-Dilemma), wird in Art. 25 zur durchsetzbaren Rechtspflicht.

DEFINITION

Privacy by Design (Datenschutz durch Technikgestaltung)

Der Datenschutz muss bereits bei der initialen Softwareentwicklung und Systemkonzeption von Beginn an als Kernelement implementiert werden, etwa durch strikte Zugriffsrestriktionen, Pseudonymisierung oder eine datensparsame Architektur.

DEFINITION

Privacy by Default (datenschutzfreundliche Voreinstellungen)

Eine Software oder App muss in ihrer konfigurativen Grundeinstellung den maximal datenschutzfreundlichen Zustand bieten. Nur die für den konkreten Zweck erforderlichen Daten dürfen *standardmäßig* ohne aktives Zutun der Nutzerin verarbeitet werden.

Dieses Leitbild ist in der Praxis hart umkämpft. Ein Cookie-Banner, das Vorauswahlen für Werbe-Cookies trifft oder bei dem „Alles akzeptieren" prominent hervorgehoben und leichter zu klicken ist als „Alles ablehnen", steht im klaren Konflikt mit Privacy by Default. Dennoch sind solche Banner weit verbreitet. Sie zeigen exemplarisch, dass die rechtliche Pflicht und die wirtschaftlichen Anreize der Datenverarbeiter regelmäßig auseinanderfallen.

03

KAPITEL

Wenn der Schutz versagt: Meldepflichten bei Datenpannen

Trotz aller Maßnahmen kann es zu einer **Verletzung des Schutzes personenbezogener Daten** kommen, einem „personal data breach", etwa durch einen Hackerangriff, einen Ransomware-Befall oder einen verlorenen Firmenlaptop. Die DSGVO reagiert darauf mit einem zweistufigen Meldesystem.

Art. 33 DSGVO verpflichtet den Verantwortlichen, eine Datenpanne der zuständigen Aufsichtsbehörde *unverzüglich, möglichst binnen 72 Stunden* nach Bekanntwerden zu melden. Hiervon ist nur dann eine Ausnahme möglich, wenn die Verletzung voraussichtlich *nicht* zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt. Die Meldung muss Art und Umfang der Panne, die wahrscheinlichen Folgen und die ergriffenen Gegenmaßnahmen beschreiben.

Art. 34 DSGVO verlangt zusätzlich die *Benachrichtigung der betroffenen Personen selbst*, allerdings nur, wenn die Verletzung voraussichtlich ein *hohes Risiko* für deren Rechte und Freiheiten zur Folge hat. Die Schwelle ist hier also höher als bei der Behördenmeldung: Nicht jede Panne

muss den Betroffenen mitgeteilt werden, wohl aber jede gravierende. Die Benachrichtigung kann unterbleiben, wenn die betroffenen Daten etwa durch Verschlüsselung wirksam unzugänglich bleiben. Das ist ein weiterer Anreiz für gute TOMs.

ÜBUNG · BEGRIFFE

Unternehmen müssen ihre Systeme nach dem Stand der **Technik** absichern. Bei riskanten Verarbeitungen ist vorab zwingend eine **Datenschutz-Folgenabschätzung** durchzuführen. Kommt es zu einem Hack, muss der Vorfall binnen **72** Stunden an die Behörde gemeldet werden.

04

KAPITEL

Die regulierte Selbstkontrolle: der Datenschutzbeauftragte

Um der DSGVO Wirkmacht zu verleihen, etabliert das Gesetz ein mehrstufiges Kontrollsystem aus interner Beaufsichtigung, behördlicher Aufsicht und direkter zivilrechtlicher Inanspruchnahmemöglichkeit. An vorderster Front agiert das Organ der **regulierten Selbstkontrolle**: der Datenschutzbeauftragte (DSB).

Gemäß Art. 37 DSGVO ist die Benennung eines DSB obligatorisch, wenn die Kerntätigkeit in der umfangreichen, regelmäßigen und systematischen Überwachung von Personen oder in der umfangreichen Verarbeitung besonderer Datenkategorien besteht, sowie generell für alle Behörden und öffentlichen Stellen. In Deutschland verschärft § 38 BDSG diese Pflicht erheblich: Ein DSB ist hier bereits dann zu bestellen, wenn in der Regel *mindestens 20 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Der DSB agiert organisationsrechtlich in einer bemerkenswerten Sonderrolle: Er ist fachlich weisungsfrei, berichtet unmittelbar an die höchste Managementebene und genießt gesetzlichen Kündigungsschutz. Seine primäre Aufgabe ist die Überwachung der Einhaltung der DSGVO und die strukturierte Beratung der Geschäftsführung. Er ist jedoch *nicht* originär weisungsbefugt: Die rechtliche Verantwortung für die Compliance verbleibt bei den operativ tätigen Organen des Unternehmens. Genau aus dieser Unabhängigkeit folgt ein wichtiges Verbot von Interessenkonflikten: Wer die Verarbeitung selbst bestimmt, kann sie nicht zugleich unabhängig kontrollieren.

Prüfen Sie anhand des folgenden interaktiven Schemas, ob für ein konkretes Unternehmen eine juristische Pflicht zur Benennung eines DSB besteht:

QUICK-CHECK

Dürfen Sie als Geschäftsführer eines Start-ups gleichzeitig als betrieblicher Datenschutzbeauftragter Ihres eigenen Unternehmens agieren?

Ja, sofern ich ausreichendes Fachwissen nachweise und die Behörde zustimmt.
Nein, diese Konstellation führt zwingend zu einem Interessenkonflikt. Der Geschäftsführer kann sich nicht selbst unabhängig kontrollieren.
Ja, Start-ups unter 20 Beschäftigten sind von der Trennung befreit.

05
KAPITEL

Durchsetzung von außen: Aufsichtsbehörden, Bußgelder und Haftung

Flankiert wird die interne Selbstkontrolle durch die externe Schlagkraft der **Aufsichtsbehörden**. Nach Art. 51 ff. DSGVO richtet jeder Mitgliedstaat eine oder mehrere unabhängige Aufsichtsbehörden ein. So sind beispielsweise in Deutschland die Landesdatenschutzbeauftragten sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Ihre in Art. 58 geregelten Untersuchungs- und Abhilfebefugnisse sind weitreichend: Die Palette reicht von Verwarnungen über bindende Anweisungen bis zum vollständigen Verbot einer Verarbeitung.

5.1 Der „One-Stop-Shop" und das Forum Shopping

Für grenzüberschreitend tätige Unternehmen sieht die DSGVO den **One-Stop-Shop**-Mechanismus vor: Federführend ist die Aufsichtsbehörde am Ort der Hauptniederlassung des Unternehmens. Genau dieser Mechanismus hat in der Praxis zu einem Phänomen geführt, das als **Forum Shopping** kritisiert wird: Viele große Tech-Konzerne (etwa Meta, Google, Apple) haben ihren europäischen Hauptsitz in Irland. Mit der Folge, dass die irische **Data Protection Commission (DPC)** für sie zentral zuständig wurde und ihr eine Schlüsselrolle bei der Durchsetzung gegen die größten Datenverarbeiter zufällt. Ihre Durchsetzungspraxis muss man jedenfalls in der Vergangenheit als sehr zurückhaltend bezeichnen…

5.2 Die Geldbußen (Art. 83 DSGVO)

Die schärfste Waffe der Behörden sind die Geldbußen des Art. 83 DSGVO. Das Gesetz kennt zwei Bußgeldrahmen: Bei Verstößen gegen formelle Pflichten (z. B. Art. 25, 30, 32) drohen Geldbußen von bis zu 10 Millionen Euro oder bis zu 2 Prozent des weltweiten Jahresumsatzes; bei Verstößen gegen die Grundsätze und Betroffenenrechte (Art. 5, 6, 9, 12–22) sind es bis zu 20 Millionen Euro oder – für Konzerne entscheidend – bis zu 4 Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag *höher* ist. Bemerkenswert ist, dass Bußgelder im Unternehmensverbund konsequent auf Basis des gesamten Konzernumsatzes berechnet werden. Ausgesprochene Re-

kordstrafen wie gegen Meta (1,2 Milliarden Euro, 2023, wegen rechtswidriger Datenübermittlung in die USA) oder gegen TikTok (530 Millionen Euro, 2025) verdeutlichen die reale Schlagkraft dieses Instruments.

5.3 Der Schadensersatzanspruch (Art. 82 DSGVO)

Die Durchsetzung verlagert sich zunehmend auch auf die Ebene der Betroffenen selbst. Gemäß Art. 82 DSGVO kann jede Person, der durch einen Verstoß ein materieller *oder immaterieller* Schaden entstanden ist, direkt vom Verantwortlichen Schadensersatz verlangen. Voraussetzung sind ein kausaler Verstoß (etwa lückenhafte Datensicherheit nach Art. 32) und ein konkreter Schaden. Der EuGH hat in der Leitentscheidung **„Österreichische Post" (C-300/21)** entschieden, dass ein Schadensersatzanspruch drei kumulative Voraussetzungen hat – einen Verstoß, einen Schaden und einen Kausalzusammenhang – und dass es *keine Erheblichkeitsschwelle* gibt: Auch ein geringfügiger immaterieller Schaden ist grundsätzlich ersatzfähig.

DEEP DIVE Reicht bloße „Sorge" als immaterieller Schaden?

Nach der EuGH-Judikatur kann bereits der bloße, *nachgewiesene* Kontrollverlust über persönliche Daten einen ersatzfähigen immateriellen Schaden begründen. Auch die begründete Befürchtung eines Datenmissbrauchs kann genügen. Eine völlig abstrakte „Sorge" ohne nachweisbaren tatsächlichen Eingriff reicht demgegenüber regelmäßig *nicht*. Eine generelle „Erheblichkeitsschwelle" gibt es jedoch laut EuGH ausdrücklich nicht. Die nationalen Gerichte müssen die Höhe nach den Umständen des Einzelfalls bemessen.

Welche praktische Sprengkraft Art. 82 entfaltet, zeigt der **Facebook-Scraping-Fall**: 2021 wurden Daten von über 500 Millionen Facebook-Nutzern durch Ausnutzen einer Funktion abgegriffen und öffentlich verbreitet. In der Folge klagten zahllose Betroffene in Deutschland auf immateriellen Schadensersatz. Der BGH hat im ersten **Leitentscheidungsverfahren** überhaupt nach § 552b ZPO (BGH, Urt. v. 18.11.2024 – VI ZR 10/24) klargestellt, dass bereits der durch den Kontrollverlust ausgelöste Zustand einen ersatzfähigen immateriellen Schaden darstellen kann, ohne dass ein konkreter Missbrauch nachgewiesen werden muss. Den Schaden für den bloßen, kurzzeitigen Kontrollverlust hat er beispielhaft auf rund 100 Euro beziffert. Dieses neue Verfahren erlaubt es dem BGH, eine Rechtsfrage für eine Vielzahl gleichgelagerter Fälle verbindlich zu klären. Genau das macht den Anspruch massentauglich und aus Sicht der Verantwortlichen für die Datenverarbeitung äußerst unangenehm.

5.4 Straftatbestände: § 42 BDSG und §§ 201 ff. StGB

Über die verwaltungsrechtlichen Bußgelder und den zivilrechtlichen Schadensersatz hinaus kennt das Recht auch *strafrechtliche* Sanktionen. § 42 BDSG stellt es unter Strafe, personenbezogene Daten einer großen Zahl von Personen, die nicht allgemein zugänglich sind, gegen Entgelt oder in Bereicherungs- bzw. Schädigungsabsicht unbefugt zu übermitteln oder zugänglich zu machen. Flankiert wird dies durch die Tatbestände zum Schutz des persönlichen Lebens- und Geheimbereichs im StGB, insbesondere § 201 StGB (Verletzung der Vertraulichkeit des Wortes) und § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen). Diese

Vorschriften bilden zugleich eine erste Brücke zum Strafrecht, das uns in der nächsten Einheit ausführlicher begegnen wird.

FALLSTUDIE

Fall: Das unverschlüsselte Krankenhausnetzwerk

Das renommierte Krankenhaus K speichert digitale Patientenakten auf einem unverschlüsselten, firmenintern frei zugänglichen Netzwerklaufwerk. Ein Praktikant kopiert die höchst sensiblen Daten aus bloßer Neugierde auf einen USB-Stick und verliert diesen noch am selben Abend im Regionalexpress. Nach internen Beratungen meldet die Klinikleitung den Vorfall erst nach fünf Tagen an die zuständige Datenschutzbehörde. Welche Pflichtenverstöße liegen vor, und welche Folgen drohen?

Lösung. Hier kumulieren mehrere Verstöße:

1. **Art. 32 (TOMs):** K hat eklatant gegen die Pflicht zu angemessenen Sicherheitsmaßnahmen verstoßen. Bei Gesundheitsdaten (besondere Kategorie nach Art. 9) sind Verschlüsselung und strikte Zugriffskontrolle praktisch zwingend. Das unverschlüsselte, frei zugängliche Laufwerk verletzt den Stand der Technik.
2. **Art. 33 (Meldepflicht):** Die Meldung nach fünf Tagen erfolgte zu spät. Sie hätte unverzüglich, möglichst binnen 72 Stunden, erfolgen müssen, da durch den Verlust von Gesundheitsdaten offensichtlich ein hohes Risiko besteht. Wegen dieses hohen Risikos wäre zudem nach **Art. 34** eine Benachrichtigung der betroffenen Patienten erforderlich.
3. **Sanktionen von zwei Seiten:** Die Aufsichtsbehörde dürfte wegen des strukturellen Versagens im Umgang mit Gesundheitsdaten ein hohes Bußgeld nach **Art. 83** verhängen. Gleichzeitig können die betroffenen Patienten nach **Art. 82** Schadensersatz wegen des Kontrollverlusts über ihre Gesundheitsdaten verlangen – nach der EuGH-Rechtsprechung ohne Erheblichkeitsschwelle.
4. **Strafrechtliche Dimension:** Patientendaten unterliegen der ärztlichen Schweigepflicht; ihre Offenbarung kann nach **§ 203 StGB** (Verletzung von Privatgeheimnissen) strafbar sein. Das unverschlüsselte, frei zugängliche Laufwerk, das einem Praktikanten den Zugriff überhaupt erst ermöglichte, zeigt, wie organisatorisches Versagen und strafrechtliche Risiken ineinandergreifen.

06

KAPITEL

Einzelfrage: Videoüberwachung

Ein praktisch besonders häufiger Konfliktfall ist die **Videoüberwachung**. Sie verarbeitet personenbezogene Daten (Bildaufnahmen identifizierbarer Personen) und braucht daher eine Rechtsgrundlage. Für die Überwachung durch *nicht-öffentliche* Stellen war früher § 4 BDSG die zentrale Norm. Das Bundesverwaltungsgericht hat jedoch entschieden, dass § 4 BDSG auf private Betreiber wegen des Anwendungsvorrangs der DSGVO *nicht anwendbar* ist: Die mitgliedstaatliche Öffnungsklausel des Art. 6 Abs. 2 DSGVO erfasst nur Verarbeitungen im öffentlichen Interesse

(Art. 6 Abs. 1 lit. e), nicht aber die private Videoüberwachung. Für diese ist die DSGVO unmittelbar und abschließend maßgeblich (BVerwG, Urt. v. 27.03.2019 – 6 C 2.18). Für *öffentliche* Stellen bleibt § 4 BDSG dagegen anwendbar.

Rechtsgrundlage für die private Videoüberwachung ist daher in aller Regel das **berechtigte Interesse** nach Art. 6 Abs. 1 lit. f DSGVO. Und wir wissen ja schon, dass dies eine Abwägung erfordert: Der Betreiber muss ein berechtigtes Interesse verfolgen (etwa Schutz vor Diebstahl oder Vandalismus), die Überwachung muss zur Wahrung dieses Interesses *erforderlich* sein (kein milderes Mittel verfügbar), und das Interesse darf die Grundrechte der Gefilmten nicht überwiegen. In der Praxis folgt daraus: Eine flächendeckende, dauerhafte Überwachung von Publikumsbereichen ist meist unverhältnismäßig; zulässig ist regelmäßig nur die zweckgebundene Überwachung neuralgischer Punkte (etwa des Kassenbereichs statt des gesamten Ladens).

Hinzu treten zwei flankierende Pflichten, die in der Praxis oft entscheiden: Erstens trifft den Betreiber eine **Hinweispflicht**. Die Kameraüberwachung ist eine Verarbeitung, über die nach Art. 13 DSGVO (den uns schon bekannten Informationspflichten) zu informieren ist. Üblich ist das von den Aufsichtsbehörden empfohlene zweistufige Modell: ein gut sichtbares Kamera-Piktogramm mit den Kerninformationen bereits *vor* dem überwachten Bereich, ergänzt um die vollständigen Informationen (Verantwortlicher, Zweck, Speicherdauer, Betroffenenrechte) auf einer zweiten Stufe. Zweitens gilt das Gebot kurzer **Speicherfristen**: Als Faustregel der Aufsichtspraxis sind Aufzeichnungen regelmäßig binnen *48 bis 72 Stunden* zu löschen; eine längere Speicherung bedarf eines konkreten Anlasses (etwa eines dokumentierten Vorfalls). Wo eine systematische weiträumige Überwachung öffentlich zugänglicher Bereiche vorliegt, ist sie überdies ein Regelbeispiel der DSFA (Art. 35).

QUICK-CHECK

Worauf stützt sich ein privater Einzelhändler heute typischerweise, wenn er seinen Verkaufsraum per Kamera überwacht?

Auf eine Einwilligung jedes einzelnen Kunden nach Art. 6 Abs. 1 lit. a
Auf das berechtigte Interesse nach Art. 6 Abs. 1 lit. f, nach einer Abwägung mit den Persönlichkeitsrechten der Gefilmten
Auf § 4 BDSG als abschließende und vorrangige Spezialnorm
Auf eine gesetzliche Pflicht zur Überwachung

07
KAPITEL

Ausblick: von der Datensicherheit zum Informationssicherheitsrecht

Das Datenschutzrecht mag an vielen Stellen bürokratisch wirken. Wer es jedoch ignoriert, riskiert empfindliche Bußgelder, Schadensersatzklagen und im Extremfall strafrechtliche Verfolgung. Die Investition in saubere Compliance ist letztlich nichts anderes als präventives Risikomanagement.

ÜBUNG · BEGRIFFE

Zur internen Überwachung ist häufig ein unabhängiger **Datenschutzbeauftragter** zu bestellen. Auf Behördenebene sanktioniert die DSGVO Versäumnisse mit scharfen **Geldbußen**. Zusätzlich können betroffene Personen bei nachweisbarem Kontrollverlust direkt auf **Schadensersatz** klagen.

Mit der Datensicherheit aus Art. 32 DSGVO haben wir zugleich die Brücke zur nächsten Einheit geschlagen. Denn die Pflicht, IT-Systeme nach dem Stand der Technik gegen Angriffe und Ausfälle zu härten, ist nicht auf personenbezogene Daten beschränkt. In der kommenden Lerneinheit zum **Informationssicherheitsrecht** weiten wir den Blick: Wir betrachten den Schutz *kritischer Infrastrukturen* (KRITIS), die unionsrechtlichen Vorgaben der **NIS2-Richtlinie** und ihre Umsetzung im BSIG sowie das **IT-Strafrecht** der §§ 202a ff. StGB. Wo der Datenschutz die natürliche Person schützt, schützt das Informationssicherheitsrecht die Funktionsfähigkeit der digitalen Systeme selbst. Art. 32 DSGVO ist der Punkt, an dem beide Welten zusammenfinden.

08
KAPITEL

Quellen

8.1 Normen & Standards

- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), insb. Art. 24, 25, 30, 32, 33, 34, 35, 36, 37, 51 ff., 58, 82, 83. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679
- Bundesdatenschutzgesetz (BDSG), insb. § 4 (Videoüberwachung), § 38 (Benennung eines Datenschutzbeauftragten), § 42 (Strafvorschriften). https://www.gesetze-im-internet.de/bdsg_2018/

- Strafgesetzbuch (StGB), §§ 201, 201a (Verletzung der Vertraulichkeit des Wortes / des höchstpersönlichen Lebensbereichs). https://www.gesetze-im-internet.de/stgb/
- Standard-Datenschutzmodell (SDM) – Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

8.2 Rechtsprechung

- EuGH, Urteil vom 04.05.2023 – C-300/21 (Österreichische Post), zum immateriellen Schadensersatz nach Art. 82 DSGVO und zur fehlenden Erheblichkeitsschwelle.
- BGH, Urteil vom 18.11.2024 – VI ZR 10/24 (Facebook-Scraping), zum ersatzfähigen Kontrollverlust nach Art. 82 DSGVO; erstes Leitentscheidungsverfahren nach § 552b ZPO.
- BVerwG, Urteil vom 27.03.2019 – 6 C 2.18 (Videoüberwachung), zur Unanwendbarkeit des § 4 BDSG auf nicht-öffentliche Stellen wegen Anwendungsvorrangs der DSGVO.