thws Technische Hochschule Würzburg-Schweinfurt

FAKULTÄT INFORMATIK UND WIRTSCHAFTSINFORMATIK

VORLESUNGSSKRIPT

Datenschutzrecht

Technik, Organisation und Durchsetzung

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

01
KAPITEL

Datenschutzcompliance in der Praxis

Das fortschrittlichste Datenschutzrecht bleibt ein zahnloser Tiger, solange es nicht durch robuste Technik und organisatorishe Maßnahmen flankiert und vor allem schlagkräftig durchgesetzt wird. Die DSGVO belässt es daher nicht bei abstrakten Vorgaben zur rechtmäßigen Verarbeitung, sondern zwingt Unternehmen zur proaktiven technischen Absicherung ihrer Systeme. Wer bei der Compliance spart, dem drohen empfindliche Sanktionen. Diese Einheit skizziert die organisatorischen und technischen Pflichten und beleuchtet das scharfe Sanktionsregime Europas.

1.1 Technischer und organisatorischer Datenschutz

In der betrieblichen Praxis konvergieren die Welten der IT-Sicherheit und der Datenschutz-Compliance, auch wenn sie juristisch zu trennen sind. Die Datensicherheit (Informationssicherheit) zielt institutionell auf den Schutz von Hardware, Software und Datenbeständen gegen Verlust, Zerstörung oder Missbrauch durch Unbefugte. Der Datenschutz hingegen nimmt zwingend die natürliche Person ins Visier und schützt sie vor Persönlichkeitsrechtsverletzungen. Ihre zentrale Schnittmenge bildet Art. 32 DSGVO betreffend die 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.

DEEP DIVE Der “Stand der Technik” und das SDM

Maßgeblich für die Beurteilung der IT-Sicherheitsmaßnahmen ist der „Stand der Technik“. Dieser Begriff meint den Entwicklungsstand fortschrittlicher Verfahren, die sich in der Praxis bewährt haben – in Abgrenzung zum rudimentären „Stand der allgemeinen Praxis“ oder dem noch unerprobten „Stand der Wissenschaft“ - wäre dies gefordert, müssten Sie deutlich mehr tun, als nur etablierte Industriestandards umzusetzen.
Zur konzeptionellen Umsetzung dient in der behördlichen Praxis häufig das Standard-Datenschutzmodell (SDM). Es definiert 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 völlig unterschiedliche Zwecke erhoben wurden, unzulässig zusammengeführt werden. Das SDM spezifiziert diese Ziele weiter in konkrete Anforderungen an die Systemarchitektur und die Verarbeitungsprozesse. Die jeweils aktuelle Fassung findet sich auf den Webseiten des Landesbeauftragten für Datenschutz und Infromationsfreiheit Mecklenburg-Vorpommern

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

1.1.1 Privacy by Design und Privacy by Default

Ein zentraler Innovationsansatz der DSGVO manifestiert sich darüber hinaus in Art. 25 DSGVO, der Softwareentwicklung und Systemarchitektur unmittelbar an rechtliche Maßstäbe bindet.

DEFINITION

Privacy by Design

Datenschutz durch Technikgestaltung. Der Datenschutz muss bereits bei der initialen Softwareentwicklung und Systemkonzeption von Beginn an als Kernelement implementiert werden (z. B. durch strikte Zugriffsrestriktionen).

DEFINITION

Privacy by Default

Datenschutz durch datenschutzfreundliche Voreinstellungen. Eine Software oder App muss in ihrer konfigurativen Grundeinstellung maximalen Datenschutz bieten.

Dieses Leitbild ist in der Praxis oft hart umkämpft. Ein Cookie-Banner, das Vorauswahlen für Werbe-Cookies trifft, oder bei dem das Feld „Alles akzeptieren“ prominent farblich hervorgehoben und leichter zu klicken ist als „Alles ablehnen“, steht im Konflikt mit den Prinzipien des Privacy by Design und Privacy by Default - dennoch sind solche Banner in der Praxis weit verbreitet.

1.1.2 Dokumentations- und Meldepflichten

Neben der technischen Härtung der Systeme überwacht die DSGVO das Gebaren der Verantwortlichen durch stringente Dokumentations- und Meldepflichten:

1. **Verzeichnis von Verarbeitungstätigkeiten (VvT):** Das operationelle Herzstück der Compliance. Art. 30 DSGVO verlangt die lückenlose Dokumentation aller Datenverarbeitungsprozesse in ihrer Organisation. Dieses Verzeichnis dient als Nachweis gegenüber den Aufsichtsbehörden und den Betroffenen, dass die Verarbeitung rechtmäßig erfolgt. Denken Sie zurück an die Ausführungen zu den Grundprinzipien der DSGVO: Sie sind als Verantwortlicher verpflichtet, die Rechtmäßigkeit der Verarbeitung nachzuweisen. Das VvT ist hierfür das zentrale Instrument.
2. **Datenschutzfolgenabschätzung (DSFA):** Ist bei einer Datenverarbeitung ein hohes Risiko für die Betroffenen zu erwarten – prominentes Beispiel ist der Einsatz von KI zur Erstellung von Scorings –, muss vorab eine strukturierte Risikobewertung durchgeführt werden (Art. 35 DSGVO).
3. **Meldepflicht bei Datenpannen:** Kommt es trotz aller Maßnahmen zu einer Verletzung des Schutzes personenbezogener Daten (Security Breach, verlorener Firmenlaptop), muss dies der Aufsichtsbehörde unverzüglich, möglichst binnen 72 Stunden, gemeldet werden (Art.

33 DSGVO), es sei denn, ein Risiko für die Rechte und Freiheiten natürlicher Personen ist unwahrscheinlich.

ÜBUNG · BEGRIFFE

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

02

KAPITEL

Durchsetzung, Kontrolle und Haftung

Um der DSGVO Wirkmacht zu verleihen, etabliert das Gesetz ein mehrstufiges und ineinandergreifendes Kontrollsystem aus interner Beaufsichtigung, umfassenden Ermächtigungen für Behördeninterventionen und direkter zivilrechtlicher Inanspruchnahme.

An vorderster Front agiert das Organ der sogenannten regulierten Selbstkontrolle: Der Datenschutzbeauftragte (DSB).

Gemäß Art. 37 DSGVO ist dessen Benennung obligatorisch, wenn die Kerntätigkeit in der Verarbeitung besonders sensibler Daten oder der umfangreichen systematischen Überwachung besteht sowie generell für alle öffentlichen Stellen. In Deutschland verschärft § 38 BDSG die Pflicht massiv: Hier ist ein DSB bereits dann zu bestellen, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung von 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 und strukturierte Beratung der Geschäftsführung. Allerdings ist er nicht originär weisungsbefugt. Die rechtliche Verantwortung für die Einhaltung der DSGVO verbleibt bei den operativ tätigen Organen des Unternehmens.

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 für Ihr eigenes Unternehmen agieren?

- ☐ Ja, sofern ich ausreichendes Fachwissen nachweisen kann und die Behörde zustimmt.
- ☑ **Nein, diese Konstellation führt rechtlich zwingend zu einem Interessenkonflikt, da sich der Geschäftsführer nicht selbst unabhängig kontrollieren kann.**
- ☐ Ja, Start-ups unter 20 Mitarbeitern sind von der strengen Trennung befreit.

Flankiert wird die interne Selbstkontrolle durch die externe Schlagkraft der unabhängigen Aufsichtsbehörden auf Landes- und Bundesebene. Deren Untersuchungs- und Abhilfebefugnisse sind überaus weitreichend. Die behördliche Palette reicht von drängenden Verwarnungen über bindende Anweisungen bis hin zum ultimativen Instrument: dem vollständigen Verbot einer Datenverarbeitung.

Die schärfste Waffe der Behörden sind jedoch die drakonischen Geldbußen des Art. 83 DSGVO. Je nach Verstoß drohen Strafen von bis zu 20 Millionen Euro oder – und das ist für Tech-Konzerne entscheidend – bis zu 4 Prozent des weltweiten Jahresumsatzes. Rekordstrafen wie gegen Meta (1,2 Milliarden Euro) oder TikTok (530 Millionen Euro) wegen rechtswidriger Datenübermittlungen nach Übersee verdeutlichen die Schlagkraft der DSGVO. Bemerkenswert ist dabei, dass Bußgelder im Unternehmensverbund konsequent auf Basis des gesamten Konzernumsatzes berechnet werden.

Die Durchsetzung verlagert sich aber zunehmend auch auf die Ebene der Betroffenen. Gemäß Art. 82 DSGVO können Bürger direkt gegen Unternehmen vorgehen und Schadensersatz verlangen.

Voraussetzung hierfür sind ein kausaler Verstoß (beispielsweise lückenhafte Datensicherheit) und ein konkreter materieller oder immaterieller Schaden. Der Bundesgerichtshof (BGH) sowie der Europäische Gerichtshof (EuGH) haben inzwischen mehrfach entschieden, dass ein Schaden nicht zwingend eine physische oder finanzielle Komponente erfordert.

DEEP DIVE Reicht “Sorge” als immaterieller Schaden?

Nach aktueller EuGH-Judikatur kann bereits der bloße, bewiesene Kontrollverlust über hochsensible persönliche Daten (z. B. das ungewollte Bekanntwerden von Gesundheitsdaten) einen ersatzfähigen immateriellen Schaden begründen. Eine bloße abstrakte „Sorge“ ohne nachweisbaren tatsächlichen Eingriff genügt demgegenüber zumeist nicht. Eine „Erheblichkeitsschwelle“ gibt es bei der DSGVO jedoch laut EuGH nicht.

Wie die unterschiedlichen Haftungsinstrumente der DSGVO im schlimmsten Fall kumulieren können, veranschaulicht der folgende Fall aus der betrieblichen Realität.

FALLSTUDIE

Fall: Das unverschlüsselte Krankenhausnetzwerk

Das renommierte Krankenhaus K speichert digitale Patientenakten auf einem unverschlüsselten, firmenintern frei zugänglichen Netzwerklaufwerk. Ein Praktikant kopiert die höchst privaten Daten aus bloßer Neugierde auf einen USB-Stick. Den Stick verliert er noch am selben Abend im Regionalexpress. Nach internen Beratungen meldet die Klinikleitung den Vorfall nach 5 Tagen an die zuständige Datenschutzbehörde.
Lösung. **Lösung:** Hier kumulieren die juristischen Katastrophen. Erstens hat K eklatant gegen die Pflichten zu angemessenen Sicherheitsmaßnahmen (Verschlüsselung, strikte Zugriffskontrolle, Verschwiegenheit) aus Art. 32 DSGVO verstoßen (*TOMs*). Zweitens erfolgte die Meldung des Breaches nach Art. 33 DSGVO viel zu spät. Sie hätte unverzüglich, möglichst aber binnen 72 Stunden, erfolgen müssen, da durch den Verlust von Gesundheitsdaten offensichtlich ein hohes Risiko für die Betroffenen entstanden ist. Drittens droht nun von zwei Seiten Gefahr: Die Aufsichtsbehörde dürfte aufgrund des fahrlässigen und strukturellen Versagens im Umgang mit Gesundheitsdaten ein sehr hohes Bußgeld gegen K verhängen. Gleichzeitig können die betroffenen Patienten nach Art. 82 DSGVO Schadensersatz wegen des schwerwiegenden Kontrollverlusts über ihre Gesundheitsdaten geltend machen.

Das Datenschutzrecht mag an vielen Stellen bürokratisch wirken. Wer es aber ignoriert, gefährdet nicht selten die betriebliche Existenz. Die Investition in saubere Architektur und 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 immensen **Geldbußen**. Zusätzlich können betroffene Personen bei nachweisbarem Kontrollverlust direkt auf **Schadensersatz** klagen.