Lernzettel

Datenschutz, Privatsphäre und Autonomie: Rechte, Schutzmechanismen und Gestaltung

Universität: Technische Universität Berlin
Kurs/Modul: Informatik und Gesellschaft

Erstellungsdatum: September 19, 2025

Lernzettel: Datenschutz, Privatsphäre und Autonomie: Rechte, Schutzmechanismen und Gestaltung

(1) Grundbegriffe: Datenschutz, Privatsphäre und Autonomie
Datenschutz bedeutet den Schutz personenbezogener Daten vor unbefugter oder willkürlicher Verarbeitung. Er umfasst auch das informationelle Selbstbestimmungsrecht, also die Kontrolle darüber, wer welche Daten wofür nutzt.
Privatsphäre bezeichnet den Schutz des Einzelnen vor unerwünschter Beobachtung und Freiraum in persönlichen Lebensbereichen.
Autonomie in der IT bedeutet die Fähigkeit und das Recht von Individuen, eigenständig über ihre digitalen Informationen und deren Nutzung zu entscheiden. Gestaltung und Technik beeinflussen diese Freiräume und damit die Handlungsfähigkeit der Nutzerinnen und Nutzer.

(2) Rechte der betroffenen Personen (DSGVO-Grundrechte)
Nach geltendem Datenschutzrecht haben Betroffene unter anderem folgende Rechte:

- Recht auf Auskunft über die gespeicherten Daten und deren Verarbeitungszwecke.
- Recht auf Berichtigung unrichtiger Daten.
- Recht auf Löschung („Recht auf Vergessenwerden“) unter bestimmten Voraussetzungen.
- Recht auf Einschränkung der Verarbeitung.
- Recht auf Datenübertragbarkeit (Daten in einem gängigen Format).
- Widerspruchsrecht gegen Verarbeitung aus Gründen der besonderen Situation, einschließlich Profiling.
- Recht auf Nichtunterfallnahme automatisierter Entscheidungsfindung mit Rechtswirkungen.

(3) Schutzmechanismen: Technische und organisatorische Maßnahmen (TOM)
Schutzmechanismen lassen sich grob in technische und organisatorische Maßnahmen unterteilen:

- Technische Maßnahmen (TM):
  - Verschlüsselung von Daten bei Speicherung und Übertragung.
  - Zugriffskontrollen, starke Authentifizierung und Least-Privilege-Prinzip.
  - Pseudonymisierung und Anonymisierung wo möglich.
  - Sicherer Umgang mit Backups und sicheren Kommunikationsprotokollen.
- Organisatorische Maßnahmen (OM):
  - Datenschutz-Folgenabschätzung (DSFA) bei risikoreichen Verarbeitungen.
  - klare Rollen- und Berechtigungsstrukturen, Schulungen, Richtlinien.
  - Dokumentation der Verarbeitungstätigkeiten und regelmäßige Audits.

(4) Gestaltung von IT-Systemen: Privacy by Design und Privacy by Default

- Privacy by Design: Datenschutz als integraler Bestandteil der Systementwicklung von Anfang an.
- Privacy by Default: Voreinstellungen standardmäßig datenschutzfreundlich.
- Datenminimierung: Erhebung nur der unbedingt notwendigen Daten.
- Zweckbindung: Klare, legitime Zwecke und Begrenzung der Speicherung.
- Transparenz: Klare Informationen über Zwecke, Rechtsgrundlagen und Empfänger.
- Nutzerfreundlichkeit und Verständlichkeit der Datenschutzinformationen (Plain Language).
- Barrierefreiheit und gleichberechtigter Zugang zu Informationen über Datenschutz.

(5) Gestaltungsethik, Verantwortlichkeit und Grundrechte im Digitalen Kontext

- Respekt vor Autonomie, Fairness und Nichtdiskriminierung.
- Offenlegung von Funktionsweisen, insbesondere bei Profiling und automatisierter Entscheidungsfindung.
- Berücksichtigung sozialer Auswirkungen von Datenerhebungen, Tracking und Verhaltensprofilen.
- Verantwortliche Gestaltung durch Informatikerinnen und Informatiker: Verantwortung, Transparenz und Rechtskonformität.

(6) Risiken, Regulierung und Technikfolgenabschätzung

- Risiken: Datenleck, ungewollte Datenteilhabe, Cross-Site-Tracking, Profiling, Missbrauch von Sensor- oder Standortdaten.
- Regulierungstypen: Datenschutzgesetze (z. B. DSGVO), branchenspezifische Vorgaben, interne Compliance.
- Datenschutz-Folgenabschätzung (DSFA) als Instrument zur Bewertung von Risiken und Gegenmaßnahmen.
- Notwendigkeit von Transparenz, Audits und Reaktionsplänen bei Sicherheitsvorfällen.

(7) Gestaltung der Praxis: Beispiele aus der Analyse von Systemen

Beispiele zeigen, wie Privatsphäre und Autonomie durch Systemdesign beeinflusst werden:

- Beispiel A: Eine Fitness-App sammelt Standort- und Gesundheitsdaten. Transparente Zweckbindung, Minimierung, Verschlüsselung und eine klare Opt-in-Entscheidung werden implementiert; Nutzerinnen und Nutzer erhalten Auskunfts- und Löschrechte.
- Beispiel B: Eine Messaging-Plattform nutzt Metadaten-Logs. Pseudonymisierung, Zugriffsbeschränkungen, regelmäßige Sicherheitsüberprüfungen und DSGVO-konforme Datenverarbeitung werden sichergestellt.

(8) Fazit: Handlungsempfehlungen für Informatikerinnen und Informatiker

- Berücksichtige Privacy-by-Design von der ersten Zeile Code bis zur Deployment-Pipeline.
- Verankere Datenschutzrechte in den Spezifikationen, Tests und der Dokumentation.
- Fördere Transparenz, Verständlichkeit und Barrierefreiheit der Datenschutzinformationen.
- Implementiere effektive TOMs, führe DSFAs durch und halte Regulierung ein.
- Fördere eine verantwortliche Kultur, die Autonomie und Privatsphäre in den Mittelpunkt stellt.