# LU12a: Datenschutz & Datensicherheit

## Lernziele

Nach dieser Unterrichtseinheit können Sie:

- den Unterschied zwischen Datenschutz und Datensicherheit erklären.
- typische Schutzmassnahmen (z. B. Verschlüsselung, Hashing, Masking, Zugriffsrechte) benennen.
- anhand von Beispielen der Berufsfachschule erklären, warum Rollen und Berechtigungen nötig sind.

# 1. Datenschutz in der Schweiz (DSG) und in der EU (DSGVO)

### Grundidee

Datenschutz bezieht sich auf den Schutz von **Personendaten**. Das Datenschutzgesetz (DSG) in der Schweiz:

- schützt Personendaten natürlicher Personen,
- stärkt die Selbstbestimmung der betroffenen Personen über ihre Daten,
- verlangt transparente, rechtmässige und verhältnismässige Datenbearbeitung.

Die DSGVO (EU) verfolgt ähnliche Ziele und ist für Schweizer Firmen relevant, wenn sie z. B.:

- Dienstleistungen oder Produkte in der EU anbieten,
- Personen in der EU systematisch beobachten (Tracking, Profiling).

#### Wer ist betroffen?

- Alle Unternehmen/Organisationen, die in der Schweiz Personendaten bearbeiten unabhängig davon, wo sie ihren Sitz haben.
- Dazu gehören auch Schulen, Verwaltungen und IT-Dienstleister.

## **Zentrale Begriffe**

Abkürzung	Bedeutung
DSG	Datenschutzgesetz Schweiz (Schutz von Personendaten)
DSV	Verordnung zum DSG (Detailbestimmungen zur Umsetzung)
DSGVO	Datenschutz-Grundverordnung der EU
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter – unabhängige Behörde, überwacht die Einhaltung der Datenschutzgesetze

# 2. Welche Daten sind geschützt?

**Personendaten** = alle Informationen über eine **identifizierte oder identifizierbare** natürliche Person, z. B.:

- Name, Adresse, Telefonnummer, E-Mail-Adresse
- Geburtsdatum, AHV-Nummer, Klassenbezeichnung
- Standortdaten, Login-Daten, IP-Adressen

### Besonders schützenswerte Personendaten (brauchen einen höheren Schutz), z. B.:

- Gesundheitsdaten (Diagnosen, Arztzeugnisse)
- religiöse oder politische Ansichten
- Daten über Strafverfahren
- genetische und biometrische Daten
- intime Aspekte der Persönlichkeit

In einer Schule gehören z. B. auch **Noten und Beurteilungen** in diese Kategorie oder sind ihr sehr nahe: Sie beeinflussen die Zukunft der Lernenden und dürfen nicht unkontrolliert verbreitet werden.

# 3. Datenklassifikation - wie kritisch sind welche Daten?

Um geeignete Schutzmassnahmen zu wählen, werden Daten oft in Klassen eingeteilt:

### Sensitive Daten

- können einer Person direkt schaden
- o Beispiele: PIN, Passwörter, Gesundheitsdaten

## • Vertrauliche Daten

Geschäftsgeheimnisse, interne Strategien

### Kritische Daten

- für den Betrieb überlebenswichtig
- Beispiel: Finanzdaten eines Unternehmens, zentrale Benutzerverzeichnisse

#### Private Daten

• Adressen, Telefonnummern, persönliche Infos von Lernenden

#### Öffentliche Daten

o z. B. Marketingtexte auf der Website, trotzdem Schutz vor Änderung durch Dritte nötig

#### Restriktive Daten

- nur für wenige berechtigte Personen
- Beispiele: Lohnlisten, Notenübersichten, Dispensationsgründe

Die Berufsschule speichert solche Daten in verschiedenen Systemen, z. B.:

- Informationen über die Lernenden (Stammdaten),
- Informationen über die Mitarbeitenden und Lehrpersonen,
- Absenzen,
- Noten.
- → An diesen Stellen werden später **Rollen und Berechtigungen** wichtig: Nicht alle Personen dürfen

https://wiki.bzz.ch/ Printed on 2025/11/17 10:20

alles sehen oder ändern.

# 4. Datensicherheit: Was muss geschützt werden?

Datensicherheit beantwortet nicht primär die Frage "wer ist die Person?", sondern:

- **Vertraulichkeit** nur Befugte dürfen Daten lesen.
- Integrität Daten dürfen nicht unbemerkt und unberechtigt verändert werden.
- Verfügbarkeit Daten sind bei Bedarf verfügbar (z. B. für Zeugnisdruck, Prüfungen).

Beispiele aus dem Schulalltag:

- Vertraulichkeit: Noten sollen nicht für alle Lernenden öffentlich einsehbar sein.
- Integrität: Eine Note darf nicht "einfach so" im System verschwinden oder geändert werden.
- Verfügbarkeit: Noten müssen beim Zeugnisdruck zuverlässig vorhanden sein.

Datenschutz (rechtlicher Rahmen) und Datensicherheit (technische und organisatorische Massnahmen) gehören zusammen.

# 5. Schutztechniken im Überblick

In den nächsten Abschnitten sehen Sie typische Massnahmen zur Datensicherheit.

## 5.1 Verschlüsselung (Encryption)

Verschlüsselung macht Daten für Unbefugte **unlesbar**. Nur mit einem passenden Schlüssel können die Daten wieder im Klartext gelesen werden.

Typische Einsätze:

- Gespeicherte Daten ("data at rest"):
  - Festplatten, Datenbanken oder einzelne Dateien werden verschlüsselt gespeichert.
  - Beispiel: Laptop-Verschlüsselung wenn das Gerät gestohlen wird, bleiben die Daten geschützt.
- Übertragene Daten ("data in transit"):
  - Daten, die über ein Netzwerk gesendet werden, werden verschlüsselt übertragen.
  - Beispiele: HTTPS im Browser, VPN für den Fernzugriff.

Ziel: Wenn jemand Daten abfängt oder ein Gerät stiehlt, sollen die Inhalte trotzdem geschützt bleiben.

# 5.2 Hashing

Hashing ist eine **Einwegfunktion**:

- Aus einem Input (z. B. einem Passwort) wird ein fester, scheinbar zufälliger Wert (Hash).
- Aus dem Hash kann das ursprüngliche Passwort nicht oder nur mit extrem grossem Aufwand zurückberechnet werden.

### Typisches Einsatzgebiet:

### • Passwortspeicherung:

- Das System speichert **nicht** das Passwort selbst, sondern nur den Hash.
- Beim Login wird aus dem eingegebenen Passwort wieder ein Hash berechnet.
- Stimmen gespeicherter Hash und neu berechneter Hash überein, ist das Passwort korrekt.

Ziel: Selbst wenn jemand die Datenbank mit den Hashes stiehlt, sollen die eigentlichen Passwörter nicht direkt lesbar sein.

### 5.3 Weitere Bausteine der Datensicherheit

### • Zugriffskontrollen (Access Control)

- Legen fest, wer auf welche Daten zugreifen darf und was diese Person tun darf (lesen, ändern, löschen).
- Werden oft über **Benutzer**, **Rollen und Rechte** umgesetzt.
- Genau dieser Punkt wird in LU12b und LU12c anhand der Noten-Datenbank konkret angeschaut.

### MFA (Multi-Faktor-Authentifizierung)

- Zusätzlicher Faktor neben dem Passwort, z. B. SMS-Code, App-Bestätigung oder Hardware-Token.
- Erschwert den Zugriff für Angreifer, selbst wenn ein Passwort bekannt ist.

## • Backups & Recovery-Konzepte

- Regelmässige Sicherungen der Daten.
- Geplante und getestete Wiederherstellungsprozesse, damit Daten nach Fehlern oder Angriffen wiederhergestellt werden können.

#### Monitoring und Audits

- Protokollierung von Zugriffen und Änderungen (Logs).
- Alarme bei ungewöhnlichem Verhalten (z. B. sehr viele fehlgeschlagene Logins, Massenlöschungen).

### Segmentierung

- Trennung von Netzen und Systemen nach Sensitivität.
- Beispiele:
  - Trennung von Test- und Produktionssystemen,
  - nur bestimmte Netzbereiche dürfen überhaupt auf Datenbanken mit sensiblen Daten zugreifen.

Gerade der Punkt **Zugriffskontrollen (Wer darf was?)** ist der direkte Übergang zur nächsten Seite: Dort betrachten Sie Rollen und Zugriffe im Notenbuch-Szenario, bevor wir auf der letzten Seite die technische Umsetzung in MySQL üben.

https://wiki.bzz.ch/ Printed on 2025/11/17 10:20

# 6. Strafen & Konsequenzen bei Verstössen (Schweiz)

Verstösse gegen das DSG können ernsthafte Folgen haben:

 Bussen bis zu CHF 250'000 bei vorsätzlichen Verstössen (z. B. bewusste Weitergabe von Daten).

Der **EDÖB** (Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte) kann:

- Untersuchungen eröffnen,
- Anpassung oder Unterbrechung der Datenbearbeitung anordnen,
- im Extremfall auch die Löschung von Daten verlangen.

Für Unternehmen und Organisationen bedeutet das:

- Sensible Daten (z. B. Noten, Absenzen, Dispensationen) müssen technisch und organisatorisch gut geschützt werden.
- Es braucht klare Regeln, wer was sehen und ändern darf.
- IT-Systeme (z. B. Notenbuch, Absenzen-Tool, WebUntis, Moodle) müssen diese Regeln technisch umsetzen.

#### Merksatz für das Modul M290:

- Rechtlicher Rahmen (DSG/DSGVO) → beschreibt, was geschützt werden muss und welche Grundsätze gelten.
- Datensicherheit → beschreibt, wie Daten technisch und organisatorisch geschützt werden.

From:

https://wiki.bzz.ch/ - BZZ - Modulwiki

Permanent link:

https://wiki.bzz.ch/modul/m290\_guko/learningunits/lu12/theorie/a\_intro?rev=1763322385

Last update: 2025/11/16 20:46

