

# LU12a: Datenschutz & Datensicherheit

## Lernziele der Doppelstunde

Nach dieser Doppelstunde können Sie:

- den Unterschied zwischen Datenschutz und Datensicherheit erklären.
- typische Schutzmassnahmen (Verschlüsselung, Hashing, Masking, Rollen & Berechtigungen) benennen.
- User, Rollen und Berechtigungen in MySQL erstellen bzw. zuweisen.

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

### Grundidee

Datenschutzgesetz (DSG) Schweiz: schützt Personendaten natürlicher Personen und stärkt deren Selbstbestimmung über ihre Daten.

### Wer ist betroffen?

Alle Unternehmen/Organisationen, die in der Schweiz Personendaten bearbeiten – unabhängig vom Sitz.

### Zentrale Begriffe

Abkürzung	Bedeutung
DSG	Datenschutzgesetz Schweiz
DSV	Verordnung zum DSG (Detailbestimmungen)
DSGVO	Datenschutz-Grundverordnung der EU
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Wichtig: Die DSGVO kann auch für Schweizer Firmen gelten, z. B. wenn sie Waren/Dienstleistungen in der EU anbieten oder Personen dort überwachen.

## Welche Daten sind geschützt?

Personendaten = alle Informationen über eine identifizierte oder identifizierbare natürliche Person, z. B.: Name, Adresse, Telefonnummer, E-Mail-Adresse, Gesundheitsdaten, genetische und biometrische Daten, politische, religiöse Ansichten, ethnische Herkunft, Daten zu Verhalten und Persönlichkeit (Interessen, Konsum, Standortdaten)

Besonders schützenswerte Personendaten<sup>1)</sup> (DSG & DSGVO) brauchen höheren Schutz.

## Datenklassifikation

- Sensitive Daten – können einer Person direkt schaden → z. B. PIN, Gesundheitsdaten
- Vertrauliche Daten – Geschäftsgeheimnisse, interne Strategien
- Kritische Daten – für den Betrieb überlebenswichtig → z. B. Finanzdaten der Schule
- Private Daten – Adressen, Telefonnummer, persönliche Infos von Lernenden (DSG/DSGVO!)
- Öffentliche Daten – z. B. Marketingtexte, aber trotzdem Integritätsschutz
- Restriktive Daten – nur für definierte Rollen (z. B. Lohnlisten, Notenübersichten)

Die Berufsschule speichert auch solche Daten in verschiedenen Datenbanksystemen bzw. Softwares. Solche Daten landen in Tabellen wie schueler, mitarbeitende, loehne, noten, absenzen. → Hier braucht es klare Rollen & Berechtigungen.

## Datensicherheit: Was muss geschützt werden?

Datensicherheit fokussiert nicht auf „wer ist die Person?“, sondern auf:

- Vertraulichkeit – nur Befugte dürfen lesen.
- Integrität – Daten dürfen nicht unbemerkt verändert werden.
- Verfügbarkeit – Daten sind bei Bedarf verfügbar (Backups, Ausfallsicherheit).

## Schutztechniken im Überblick

### Verschlüsselung (Encryption)

macht Daten für Unbefugte unlesbar.

Einsatz:

- Gespeicherte Daten: Verschlüsselung von Tabellen, Dateien oder ganzen Disks.
- Daten werden verschoben: TLS/SSL (https:), VPN. *Beispiel MySQL (vereinfacht):*

```
CREATE TABLE sensitive_data( id INT AUTO_INCREMENT
PRIMARY KEY, encrypted_data VARBINARY(255) );

INSERT INTO sensitive_data(encrypted_data)
VALUES (AES_ENCRYPT('geheime_info', 'encryption_key'));

SELECT id,
AES_DECRYPT(encrypted_data, 'encryption_key') AS klartext
FROM sensitive_data;
```

==== Hashing ==== einweg-Funktion → aus Input entsteht ein fester Hash-Wert.

Originaldaten können aus dem Hash nicht zurückgerechnet werden. Typisches Einsatzgebiet: Passwortspeicherung.

```
CREATE TABLE users ( id INT AUTO_INCREMENT PRIMARY KEY,
username VARCHAR(50) UNIQUE, password_hash VARBINARY(255)
);

INSERT INTO users(username, password_hash)
VALUES ('user1', SHA2('Passwort123!', 256));

SELECT username
FROM users
WHERE password_hash = SHA2('Passwort123!', 256);
```

==== Weitere Bausteine der Datensicherheit ==== \* Zugriffskontrollen: Benutzer, Rollen, Rechte (auf folgenden Seite). \* MFA (Multi-Faktor-Authentifizierung). \* Backups & Recovery-Konzepte. \* Monitoring und Audits: Logfiles, Alarme bei ungewöhnlichen Zugriffen. \* Segmentierung: Trennung von Netzen und Datenbanken nach Sensitivität. ===== Strafen & Konsequenzen bei Verstößen (Schweiz) ===== Privatpersonen: Bussen bis zu CHF 250'000 (bei vorsätzlichen Verstößen). Unternehmen: Bussen bis CHF 50'000, wenn die verantwortliche Person nicht zumutbar ermittelbar ist. EDÖB<sup>2)</sup> kann Untersuchungen eröffnen und z. B. anordnen: \* Anpassung oder Unterbrechung der Datenbearbeitung, \* Löschung von Daten.



Merksatz für das Modul: Rechtlicher Rahmen (DSG/DSGVO) → konkrete Anforderungen → wir setzen sie technisch mit Rollen, Berechtigungen, Verschlüsselung und sauberen Konzepten im RDBMS um.

1)

erkläre was das ist

2)

erklären

From:

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

Permanent link:

[https://wiki.bzz.ch/modul/m290\\_guko/learningunits/lu12/theorie/a\\_intro?rev=1763313103](https://wiki.bzz.ch/modul/m290_guko/learningunits/lu12/theorie/a_intro?rev=1763313103)

Last update: 2025/11/16 18:11

