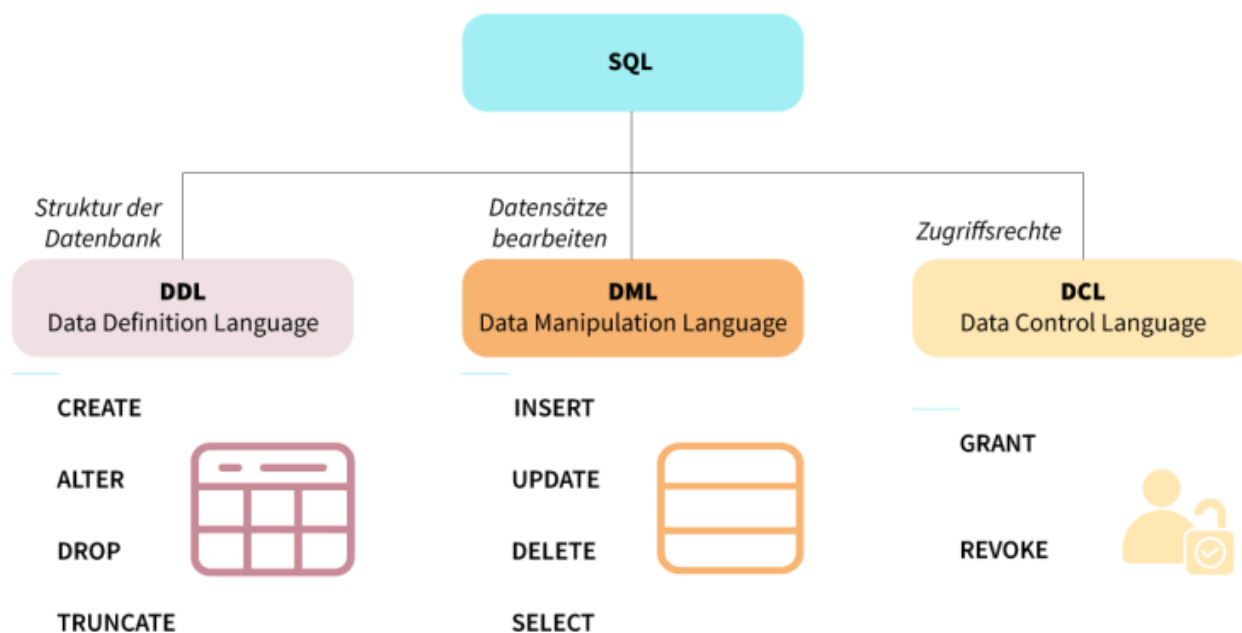


LU12a: Datenschutz & Datensicherheit



SQL-Sublanguages:

- DDL (CREATE, ALTER, DROP, TRUNCATE)
- DML (INSERT, UPDATE, DELETE, SELECT)
- DCL (GRANT, REVOKE).

Bisher haben wir DDL-Befehle (Datenbanken und Tabellen erstellen, ändern, löschen) und DML (Daten in Tabellen einfügen, ändern, löschen, auslesen) kennengelernt. Nun folgen die Berechtigungsbefehle DCL mit denen wir Berechtigungen einzelnen Usern oder Rollen zuweisen können. Der Befehl TRUNCATE gehört zur **DDL (Data Definition Language)**, weil er – im Gegensatz zu DELETE – die **Struktur einer Tabelle auf Definitionsebene verändert**. TRUNCATE löscht **alle Daten einer Tabelle**, ohne jede Zeile einzeln zu protokollieren, und setzt interne Zähler (z. B. AUTO_INCREMENT) zurück. Damit verändert er die **Tabellendefinition** im Systemkatalog.

Lernziele

Nach dieser Unterrichtseinheit können Sie:

- den Unterschied zwischen **Datenschutz** und **Datensicherheit** erklären.
- typische Schutzmassnahmen (z. B. Verschlüsselung, Hashing, Zugriffsrechte) benennen.
- anhand von Beispielen 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** – also von Daten, die etwas über eine bestimmte Person aussagen.

Das Datenschutzgesetz (DSG) in der Schweiz:

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

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

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

Wer ist betroffen?

- Alle Unternehmen und 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?

In der Praxis verwenden Organisationen oft ein eigenes Klassifikationsschema, um zu entscheiden, **wie stark** Daten geschützt werden müssen. Für die Schule kann z. B. folgendes Modell verwendet werden:

- **Sensitive Daten**
 - können einer Person direkt schaden
 - Beispiele: PIN, Passwörter, Gesundheitsdaten
- **Vertrauliche Daten**
 - nicht für die breite Öffentlichkeit bestimmt
 - Beispiele: interne Strategien, Protokolle, Bewerbungsunterlagen
- **Kritische Daten**
 - für den Betrieb überlebenswichtig
 - Beispiele: zentrale Benutzerverzeichnisse, wichtige Finanzdaten
- **Private Daten**
 - persönliche Infos von Lernenden und Mitarbeitenden
 - Beispiele: Adressen, Telefonnummern, Klassenlisten
- **Öffentliche Daten**
 - sind bewusst nach aussen sichtbar
 - Beispiele: Marketingtexte auf der Website, Modulbeschriebe
 - trotzdem Schutz vor unberechtigter Änderung nötig
- **Restriktive Daten**
 - nur für wenige berechnigte Personen
 - Beispiele: Lohnlisten, detaillierte Notenübersichten, Dispensationsgründe

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

- Informationen über die Lernenden (Stammdaten),
- Informationen über Mitarbeitende und Lehrpersonen,
- Absenzen,
- Noten.

An diesen Stellen werden später **Rollen und Berechtigungen** wichtig: Nicht alle Personen dürfen alles sehen oder ändern. Genau das bereiten wir mit LU12a vor und vertiefen es in LU12b (Rollen im Notenbuch) und LU12c (MySQL-Rollen).

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 Unterricht, Prüfungen, Zeugnisse).

Beispiele aus dem Schulalltag:

- Vertraulichkeit: Noten sollen nicht für alle Lernenden öffentlich einsehbar sein.
- Integrität: Eine Note darf nicht „einfach so“ verschwinden oder geändert werden, ohne dass man nachvollziehen kann, wer dies getan hat.
- Verfügbarkeit: Noten müssen beim Zeugnisdruck zuverlässig vorhanden sein.

Datenschutz (rechtlicher Rahmen) und Datensicherheit (technische und organisatorische Massnahmen) gehören zusammen: Das Gesetz sagt **was** zu schützen ist und welche Grundsätze gelten – die Technik und Organisation liefern das **wie**.

5. Schutztechniken im Überblick

Im Überblick einige typische Massnahmen zur Datensicherheit:

5.1 Verschlüsselung (Encryption)

Verschlüsselung macht Daten für Unbefugte **unlesbar**. Nur mit dem richtigen Schlüssel können Daten wieder im Klartext gelesen werden.

- **Gespeicherte Daten** („data at rest“): Festplatten, Datenbanken oder einzelne Dateien werden verschlüsselt gespeichert (z. B. Laptop-Verschlüsselung).
- **Übertragene Daten** („data in transit“): Daten werden beim Transport im Netzwerk verschlüsselt (z. B. HTTPS, VPN).

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

5.2 Hashing

Hashing ist eine **Einwegfunktion**:

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

Typischer Einsatz: **Passwortspeicherung** – das System speichert nur den Hash, nicht das Passwort selbst.

Ziel: Selbst wenn jemand die Datenbank mit Hash-Werten stiehlt, sollen die eigentlichen Passwörter nicht direkt lesbar sein.

5.3 Weitere Bausteine der Datensicherheit

- **Zugriffskontrollen (Access Control)**
 - Regeln, **wer** auf welche Daten zugreifen darf und **was** diese Person tun darf (lesen, ändern, löschen).
 - Werden in IT-Systemen oft über **Benutzer, Rollen und Rechte** umgesetzt.
 - Genau das ist der Schwerpunkt der nächsten Seiten (LU12b und LU12c).
- **MFA (Multi-Faktor-Authentifizierung)**
 - Zusätzlicher Faktor neben dem Passwort (z. B. SMS-Code, App-Bestätigung).
 - Erschwert Angriffe, 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. viele Fehl-Logins, Massenlöschungen).
- **Segmentierung**
 - Trennung von Netzen und Systemen nach Sensitivität.
 - Beispiele: Trennung von Test- und Produktionssystemen, nur bestimmte Netzbereiche dürfen auf sensible Datenbanken zugreifen.

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

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, unzulässige 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 (einschliesslich Schulen) 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.

Zusammenfassung:

- Datenschutz (DSG/DSGVO) sagt, **was** geschützt werden muss und welche Grundsätze gelten.
- Datensicherheit beschreibt, **wie** Daten technisch und organisatorisch geschützt werden.
- Auf den folgenden Seiten lernen Sie, wie Sie diese Anforderungen mit **Rollen, Benutzern und Berechtigungen** in einer Noten-Datenbank konkret umsetzen können.

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

Permanent link:
https://wiki.bzz.ch/modul/m290_guko/learningunits/lu12/theorie/a_intro?rev=1763327303

Last update: **2025/11/16 22:08**

