

[[TOC]]

# Modul 231 - LBV-M231-1

---

## Beruf

Informatiker/in EFZ

## Bezug zur Modulversion

[Modulversion 1](#)

## Institut

GBS St.Gallen

## Verfasser

Oliver Lux @oliver.lux

## Übersicht

Die LBV definiert drei Elemente, wobei die ersten beiden Elemente je eine schriftliche Einzelarbeit darstellen und die meisten Handlungsziele überprüfen. Das dritte Element stellt eine übergreifende Fallstudie dar, in welcher Handlungsziele praktisch an einem konkreten (wenn möglich aktuellen) Fall überprüft werden.

### Anzahl LBV-Element

3 Elemente

### Richtzeit Total (über alle Elemente)

5h

## Ergänzung

Die Gewichtung wurde so ausgestaltet, dass entweder alle LBs einfach zählen oder die Möglichkeit besteht, die 3. LB doppelt zu zählen. Mit dieser Flexibilisierung können die Bedürfnisse von mehreren BFS abgedeckt werden.

---

## Element 1

### Prüfungsform

Schriftlich

### Sozialform

Einzelarbeit

## Gewichtung

25 - 33%

## Richtzeit (Empfehlung)

1.5h

## Hilfsmittel

relevante Datenschutzgesetze, ansonsten gemäss Vorgabe der Institution

## Element Beschreibung

Die Kandidaten und Kandidatinnen kategorisieren Daten aufgrund ihres Schutzbedarfs [HZ1], überprüfen eingesetzte Anwendungen auf Einhaltung der Datenschutzgesetze [HZ4] und zeigen Konsequenzen von Fehlern im Datenschutz auf [Teil HZ 5]

## Bewertung

- Kategorisierung der schutzwürdigen Daten (35%-40%) [HZ1]
  - Unterschied Datenschutz und Datensicherheit aufzeigen
  - Unterschiedliche Rechtsräume und deren juristischen Werke aufzeigen
- Einhaltung Datenschutzgesetz und Elemente daraus (35%-40%) [HZ4]
  - Unterschiede in den einzelnen Datenschutzgesetzen der verschiedenen Rechtsräume aufzeigen
- Konsequenzen von Fehlern (20%-30%) [HZ5]
  - Erläutern der Problematik von Datenlöschung

lineare Notenskala

## Praxisbezug

Informatikerinnen und Informatiker planen Massnahmen zur Datensicherheit und zum Datenschutz, implementieren sie und dokumentieren sie:

In einem ersten Schritt identifizieren sie schutzwürdige Daten und kategorisieren sie. Als Nächstes modellieren sie die schützenswerten Daten gemäss Privacy by design. Sie klären die erforderlichen Schutzmechanismen gemäss Schutzwürdigkeit ab und qualifizieren sie. Dabei berücksichtigen sie die gesetzlichen Rahmenbedingungen (u.a. DSGVO) und interpretieren sie situationsgerecht.

- Sie identifizieren schutzwürdige Daten und kategorisieren sie. [c3.1]
- Sie informieren Kunden über Gefahren im Netz und den Umgang mit schützenswerten Daten. [b3.2]
- Sie modellieren schützenswerte Daten gemäss Privacy by design. [c3.2]

---

## Element 2

### Prüfungsform

Schriftlich, praktisch am Objekt

### Sozialform

Einzel- oder Gruppenarbeit

## Gewichtung

25 - 33%

## Richtzeit (Empfehlung)

1.5h

## Hilfsmittel

relevante Datenschutzgesetze, ansonsten gemäss Vorgabe der Institution. Keine Hilfsmittel zur Datensicherheit

## Element Beschreibung

Die Kandidaten und Kandidatinnen überprüfen und verbessern die Datensicherheit der eigenen Infrastruktur [HZ2], setzen verschiedene Möglichkeiten der Datenspeicherung ein [HZ3] und zeigen Konsequenzen von Fehlern im Datenschutz und Datensicherheit auf [HZ 5]

## Bewertung

- Bestehende Datensicherheitskonzepte überprüfen und bewerten (15%-20%) [HZ2]
  - Beschreibung Unterschied zwischen Authentifizierung und Autorisierung
- Verbesserungsmassnahmen vorschlagen (35%-40%) [HZ2]
  - Verschlüsselt Daten auf dem eigenen Rechner
  - Zeigt unterschiedliche Techniken des Zugriffsschutzes und der Passwortverwaltung auf
- Einsatz verschiedener Möglichkeiten der Datenspeicherung (15%-20%) [HZ3]
  - Zeigt Verfahren zur Speicherung von Daten und bewusst redundanter Datenhaltung auf
  - Untersucht verschiedene Gefahren, denen Daten ausgesetzt sind
- Konsequenzen bei Fehlern aufzeigen (20%-35%) [HZ5]
  - Erläutert wesentliche juristische Voraussetzungen und Eigenheiten von Websites

lineare Notenskala

## Praxisbezug

Informatikerinnen und Informatiker beraten Kundinnen und Kunden im Umgang mit schützenswerten Daten und zeigen Lösungen für Schutzmassnahmen auf. Informatikerinnen und Informatiker planen Massnahmen zur Datensicherheit und zum Datenschutz, implementieren sie und dokumentieren sie:

Sie erarbeiten ein Datensicherheits- und Rollenkonzept gemäss Auftrag, dokumentieren es und setzen es um (z.B. Backup erstellen, Zugriffsberechtigung setzen, Daten verschlüsseln).

- Sie schlagen dem Kunden nötige und empfohlene Schutzmassnahmen in den evaluierten Bereichen vor. [b3.3]
- Sie erarbeiten ein Datensicherheits- und Rollenkonzept gemäss Auftrag. [c3.4]
- Sie verschlüsseln Daten gemäss Konzept. [c3.7]
- Sie überprüfen die eingerichteten Datensicherheits- und Schutzmechanismen in Bezug auf ihre Wirksamkeit. [c3.8]

---

## Element 3

### Prüfungsform

Schriftlich, praktisch am Objekt

### Sozialform

Einzel- oder Gruppenarbeit

### Gewichtung

33 - 50%

### Richtzeit (Empfehlung)

2h

### Hilfsmittel

relevante Datenschutzgesetze, ansonsten gemäss Vorgabe der Institution. Keine Hilfsmittel zur Datensicherheit

### Element Beschreibung

Die Kandidaten und Kandidatinnen lösen eine konkrete und möglichst praxisnahe Fallstudie (evtl. aktuelle Fälle). Z.Bsp.:

- Analyse und Beurteilung bestehendes Datenschutz- und Datensicherheitskonzept
- Aufzeigen von konkreten Verbesserungsmassnahmen und Möglichkeiten zur Umsetzung beschreiben
- Auswahl von Software für die Einhaltung von Datenschutz und Datensicherheit aufgrund der Lizenzmodelle

### Bewertung

- Kategorisierung von Daten aufgrund ihres Schutzbedarfs (35%-40%) [HZ1]
  - Analyse Fallstudie bzgl. Datenschutz- oder Datensicherheitskonzept
- Überprüft und verbessert gegebenenfalls die Datensicherheit der eigenen Infrastruktur (15%-20%) [HZ2]
  - Massnahmen zur Verbesserung der kritischen Punkte aus der Fallstudie aufzeigen
- Wählt Software für die Einhaltung von Datenschutz und Datensicherheit aufgrund der Lizenzmodelle aus (40%-50%) [HZ6]
  - Mögliche Umsetzungen der Verbesserungen anhand der Fallstudie ableiten

lineare Notenskala

### Praxisbezug

Informatikerinnen und Informatiker beraten Kundinnen und Kunden im Umgang mit schützenswerten Daten und zeigen Lösungen für Schutzmassnahmen auf. Dazu klären sie zunächst mit gezielten Fragen die Sicherheitssituation bei Kundinnen und Kunden in Bezug auf System, Netzwerk, Software und Daten. Anhand

dieser Informationen schlagen sie den Kundinnen und Kunden nötige und empfohlene Schutzmassnahmen in den evaluierten Bereichen vor. Sie schaffen ein Bewusstsein für Gefahren im Netz und im Umgang mit schützenswerten Daten.

Zur Erfüllung dieser Aufgaben informieren sie sich laufend über Veränderungen der rechtlichen Rahmenbedingungen/Vorgaben.

- Sie klären anhand von gezielten Fragen die Sicherheitssituation beim Kunden in Bezug auf System, Netzwerk, Software und Daten. [b3.1]
  - Sie identifizieren schutzwürdige Daten und kategorisieren sie. [c3.1]
  - Sie schlagen dem Kunden nötige und empfohlene Schutzmassnahmen in den evaluierten Bereichen vor. [b3.3]
  - Sie schulen Mitarbeitende in der Anwendung der firmeneigenen IT-Richtlinien. [b3.4]
-