PRIVACY & LAW

FS 2025

Swiss Personal Data Protection Law (DSG)

TIME TABLE

- Why Privacy & Data Protection?
- International situation
- Legal Basis
- Principles
- Where to apply
- Rights & duties
- My TakeAway

YOUR BENEFIT – AFTER THIS LESSON YOU KNOW…

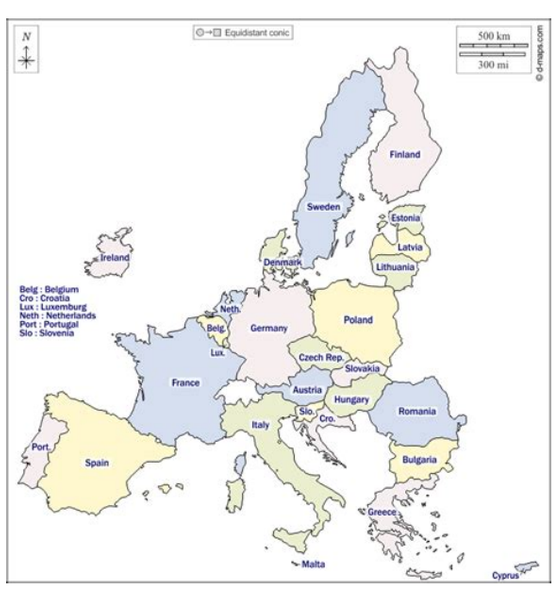
- The reasons for and the principles of Data Protection Laws
- The area of application of Data Protection Laws
- The main definitions and relevant terms
- The proceeding of the Right of Information
- The consequences if somebody doesn’t comply with the Data Protection Laws

Why Privacy & Data Protection?

- „Data Protection“ doesn’t mean protection of data - it means protecting people!
- **„Data Protection“ is part of „checks and balances“ in a functional democracy!** (control of powers).
- Humans have a **social** (public) but also an **individual** nature (privacy)! Steady conflict between these 2 natures (privacy vs. public)!
- Human learning imply making faults. Socially reminded all your life to your old faults (data trail) violates your freedom? (**right to be forgotten**)
- If you follow the idea that humans are independent - **who** decides **what** & **how** information about you will be spread?
- One of the legitimation of a government is the protection of its citizens. What when the government constantly fails in protection of privacy?
- For most companies: **huge reputation risk** if they misuse personal data! Besides of attention - **trust is everything in business!** (1973, Niklas Luhmann: „Vertrauen“)
- Someone is always making money with your data. It's about you keeping the reigns on it! (nice try - I know!)

Washington Post: Musk’s DOGE agents access sensitive personnel data, alarming security officials

Personal data exchange with other jurisdictions / Data Protection international



European Personal Data Protection

- For 41 years: **Convention 108 of the Council of Europe (1981)**. Switzerland ratified the convention (only) in 1997, therefore it is (also) CH law! Revised Convention **108+** ratified the amendment September 2023. Minimum standard for a uniform European data protection law. But also many countries (Argentina, Mexico, Morocco, Uruguay, Tunisia etc.) have ratified the convention 108+ - 31 countries actually! **Great global "radiance" for harmonisation of data protection.**

- **EU Data Protection Regulation (GDPR)**. Applies automatically to all EU countries.
  The GDPR is a minimum standard but contains so-called **"opening clauses"**, which allow country-specific, more far-reaching data protection regulations (e.g. Art. 6 para. 2 or Art. 88 para. 1 GDPR)! One must always keep an eye on the national data protection law in an EU country! For Germany, for example, this means that in employment relationships not only the GDPR applies, but also the BDSG (BundesDatenSchutzGesetz) - specifically Section 26 BDSG.

- The GDPR, which is more far-reaching than Convention 108+, has also a great "radiant power" in other parts of the world - in particular due to Art. 3 GDPR ("market place principle")! Within a short period of time after the GDPR came into force on May 25, 2018, this has led to many companies, e.g. in the USA, Australia, China and Africa (and Switzerland…), having to align themselves accordingly.

- About AI: The Swiss Federal Council want to ratify the Council of Europe Convention on Artificial Intelligence (12.02.2025)

US-American Personal Dataprotection Law

- There is no single „Federal US-Dataprotection Law", but many regulations for specific industries on US-national as well as on state level. (April 24: discussions about a «Federal American Privacy Rights Act» but already on June 27, 2024 - after „amid signals from Republicans" the legislative process had been stopped…)
- US national level: FTC (Federal Trade Commission) has issued various "Digital Privacy Laws": Cybersecurity Act, Electronics Communications Privacy Act, Computer Fraud and Abuse Act, and Economic Espionage Act.
- US national level: HIPAA (Health Insurance Portability and Accountability Act).
- California: CCPA (California Consumer Privacy Act): Addresses primarily GAFA & Co. (revenue ≥ USD 25 million, ≥ 50,000 users or profit derives ≥50% from sale of personal data). Users can prohibit disclosure of user data (revocation rule). No supervision. No regulation on transfer to third countries, etc. So far below the protection level of e.g. the GDPR!
- **Since the US data protection law does not have the level of the European data protection law** (e.g. lack of national supervision & easy accessibility for citizens to complain), the US government and the EU concluded in the year 2000 the "Safe Harbor" agreement. Switzerland did also adopted this. However, the (then) student **Max Schrems** successfully challenged the agreement at the ECJ (2015). As a result, the parties concluded the "EU-US Privacy Shield" in 2016. Schrems again challenged this agreement at the ECJ and also won in 2020 ("Schrems II ruling"). See also NOYB.eu (association founded by Schrems). October 22 President Biden signed the Executive Order „EU-U.S. Data Privacy Framework", that had been accepted by the EU in July 2023.
- Unclear under President Trump whether he will lift Biden's Executive Order or not. **Conclusion: Standard Contract Clauses with each US-Personal-Data processor…**

Chinese Personal Information Protection Law („PIPL")

- Contrary to most assumptions, the PRC does indeed have a data protection law. This "Personal Information Protection Law" - **PIPL** - came into force on 1.11.2021 and is based on the GDPR. The PIPL is applicable across borders ("market place principle") analogous to the GDPR or the Swiss revDSG.
- There are numerous open questions as to how data subjects can enforce their rights. As with the USA and other countries, the PIPL should always be seen as a possibility to enforce national interests under the pretext of "data protection".
- **Companies are strongly advised to have the data protection conditions of Chinese subsidiaries and close business relationships with a Chinese company checked by a local specialist!**

Crossboarder data transfer: either "Adequacy Decision" or "Standard Contractual Clauses"

- **Adequacy Decision** = determination by an authority (e.g. European Data Protection Board - EDSA) or CH-EDÖB that the foreign data protection law **is equivalent to its own**.
- **If personal data is transferred across borders between countries with a non-equivalent level of data protection, then these countries must agree on the mandatory EU standard contractual clauses ("Standard Contractual Clauses" - SCC, see also Art. 46 para. 2 lit. c GDPR) under contract law. This complicates/slows down the data exchange. Essentially, the foreign company undertakes to comply with the provisions of the GDPR. The transferring company, on the other hand, must adequately verify that the foreign company can technically/organisationally guarantee the protection of personal data (certification).**
- All international companies (e.g. Microsoft, Google etc.) provide such contracts. (More information for Microsoft: [HERE]

MSE | MASTER OF SCIENCE IN ENGINEERING

Judihui – Switzerland!

Some legal bases for Swiss Personal Data Protection Law

- **Swiss Constitution**
  Art. 10 Abs. 2 BV
  „Everyone has the right to personal liberty, in particular to physical and mental integrity and to freedom of movement."

  Art. 13 BV
  „1 Everyone has the right to respect for their private and family life, their home and their correspondence, post and telecommunications.

  2 Everyone has the right to protection from misuse of their personal data."

- (revised) **Swiss Federal Act on Data Protection** (Bundesgesetz über den Datenschutz, DSG). Into force since 01.09.2023 and it's Ordinance to FADP (Verordnung zum Bundesgesetz über den Datenschutz, VDSG)
- Several data-protection rules in a wide area of acts (i.e. Art. 328b CO)
- **Canton and communal**: every Canton has its own Data Protection Acts and by-laws !!

Protection of Integrity / Personality – Art. 28 CC (ZGB)

*„**Any person whose personality rights are unlawfully infringed may petition the court for protecting against all those causing the infringement.**“*
Any** infringement of the integrity/personality is **illegal!
***Unless** it is justified by the **consent of the person** whose rights are infringed or **by law** or by an **overriding private** or **public interest**. (Justifications)*

BUT:
Upon Swiss Data Protection Law (DSG) the processing of Personal Data **is in general allowed!** (Contrary to the EU-GDPR!)

Area of Application – Art. 2 revDSG

1 This Act applies to the processing of data pertaining to **natural persons** by:

a. **private persons**; (ATTENTION: „private Persons“ are natural AND legal entities!)

b. federal bodies.

2 **It does not apply to**:

a. personal data that is processed **by a natural person exclusively for personal use and which is not disclosed to outsiders**;

b. deliberations of the Federal Assembly and in parliamentary committees;

…

Territorial Scope – Art. 3 DSG

Swiss law is now also applicable in foreign countries!
(„Marktortprinzip“)

1 This Act is applicable to fact patterns that have an effect in Switzerland, even if they occurred abroad.

Example: A german company who manages Swiss pension funds also has to comply with the Swiss DSG. The german company needs therefore also a Swiss representative.

Definitions – Art. 5 DSG (1)

Art. 5 Definitions

The following definitions apply in this Act:
a. **personal data**: all information relating to an identified or identifiable natural person;
b. **data subject**: natural person whose personal data is processed;
c. **sensitive personal data**:
   1. data on religious, ideological, political or trade union-related views or activities,
   2. data on health, the intimate sphere or the racial or ethnic origin,
   3. genetic data,
   4. biometric data which unequivocally identifies a natural person,
   5. data on administrative or criminal proceedings and sanctions,
   6. data on social security measures;

d. **processing**: any operation with personal data, irrespective of the means and the procedures applied, and in particular the collection, recording, storage, use, modification, disclosure, archiving, deletion or destruction of data;
e. **disclosure**: transmitting or making personal data accessible;
f. **profiling**: any form of automated processing of personal data consisting of using such data to assess certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or whereabouts;

Definitions – Art. 5 DSG (2)

g. **High-risk profiling**: profiling which involves a high risk to the personality or fundamental rights of the data subject, as it creates a pairing between data that enables an assessment of essential aspects of the personality of a natural person;

h. **data security breach**: a security breach which leads to an unintentional or unlawful loss, deletion, destruction or modification of personal data or to personal data being disclosed or made accessible to unauthorised persons;

i. **federal body**: federal authority or service or person that is entrusted with federal public tasks;

j. **controller**: private person or federal body that alone or jointly with others decides on the purpose and the means of the processing;

k. **processor**: private person or federal body that processes personal data on behalf of the controller.

Principles – Art. 6 DSG (1)

1 Personal data must be processed **lawfully**.

2 Processing must be carried out in good faith and must be **proportionate**.

3 Personal data may only be collected **for a specific purpose which is evident to the data subject**; personal data may only be processed in a way that is compatible with such purpose.

4 It is **destroyed or anonymized** as soon as it is no longer needed with ***regard to the purpose*** of the processing.

5 Anyone who processes personal data **must ascertain that the data is accurate**. He must take all appropriate measures so that the data which is inaccurate or incomplete with regard to the purposes for which it was collected or processed is corrected, deleted or destroyed. The appropriateness of the measures depends in particular on the nature and extent of the data processing and on the risks which the processing entails for the personality and fundamental rights of the data subjects.

Principles – Art. 6 DSG (2)

6 If the consent of the data subject is required, such consent is only valid if it has been **given freely** and for one or several **specific processing activities** and **after adequate information**.

7 Consent must be given **explicitly** for:

a. the processing of sensitive personal data;

b. high-risk profiling by a private person; or

c. profiling by a federal body.

Proportionality of Data Processing – 3 Dimensions (Art. 6 Abs. 2 DSG)

Main Question:

Does the purpose really justify the processing of the personal data? Do the reason of the collected personal data justify the penetration in ones privacy?

- Which personal data is needed exactly?
- Who has access to this data?
- How long will the personal data be stored?

Data protection by Design and by Default – Art. 7 DSG

1 The controller must set up **technical and organisational measures** in order for the data processing to meet the data protection regulations and in particular the principles set out in Article 6. It considers this obligation from the planning of the processing.

2 The technical and organisational measures must be appropriate in particular with regard to the **state of the art, the type and extent of processing**, as well as the risks that the processing at hand poses to the personality and the fundamental rights of the data subjects.

3 The controller is additionally bound to ensure through appropriate pre-defined settings that the processing of the personal data is limited to the minimum required by the purpose, unless the data subject directs otherwise.

Data Security – Art. 8 DSG

1 **The controller and the processor** must ensure, through adequate technical and organisational measures, security of the personal data that appropriately addresses the risk.

2 The measures must enable the avoidance of data security breaches.

3 The Federal Council shall issue provisions on the minimum requirements for data security.

Inventory of Processing Activities – Art. 12 DSG (1)

1 The **controllers** and the **processors** each **keep an inventory of their processing activities**.

2 The **controller's inventory** contains at least the following information:

a. the controller's identity;

b. the purpose of the processing;

c. a description of the categories of data subjects and the categories of the processed personal data;

d. the categories of the recipients;

e. if possible the period of storage of the personal data or the criteria to determine the period of storage;

f. if possible a general description of the measures to guarantee data security pursuant to Article 8;

g. in case of disclosure of data abroad, the name of the state in question and the guarantees according to Article 16 paragraph 2.

Inventory of Processing Activities – Art. 12 DSG (2)

3 The processor's inventory contains information on the identity of the processor and of the controller, the categories of processing activities performed on behalf of the controller as well as the information foreseen in paragraph 2 letters f and g.

4 The federal bodies notify the FDPIC of their inventories.

5 The Federal Council provides for exceptions for companies that have less than 250 members of staff and whose processing entails only a low risk of infringing the personality of the data subject.

How do you find it out??? 🤷

Representative – Art. 14 DSG

1 Private controllers with their domicile or residence abroad **designate a representative in Switzerland** if they process personal data of persons in Switzerland and the data processing fulfils the following requirements:

a. The data processing is connected to offering goods or services in Switzerland or to monitoring the behaviour of these persons.

b. The processing is extensive.

c. It is a regular processing.

d. The processing involves a high risk for the personality of the data subjects.

2 The representative serves as a **contact point for the data subjects** and the FDPIC (EDÖB).

3 The controller publishes the name and address of the representative.

Notification of Data Security Breaches – Art. 24 DSG

1 **The controller shall notify the FDPIC as soon as possible of a data security breach that is probable to result in a high risk to the personality rights or the fundamental rights of the data subject.**

2 In the notification, it must at least indicate the nature of the data security breach, its consequences and the measures taken or foreseen.

3 **The processor shall notify the controller as soon as possible of any data security breach**.

4 The controller shall also **inform the data subject if this is necessary for the protection of the data subject** or if the FDPIC so requests.

5 It can restrict the information to the data subject, defer it or refrain from providing information if:

a. there are grounds pursuant to Article 26 paragraph 1, letter b or 2 letter b or a statutory duty of secrecy prohibits it;

b. information is impossible or requires disproportionate efforts; or

c. the information of the data subject is ensured in an equivalent manner by a public announcement.

6 A notification based on this Article can be used in criminal proceedings against the person subject to notification only with such person's consent.

Access Right – Art. 25 DSG (1)

1 **Any person may request information from the controller as to whether personal data concerning him is being processed.**

2 The data subject shall receive the information required in order to enable him to assert his rights under this Act and to ensure the transparent processing of data. **In any case, the following information is provided to the data subject:**

a. identity and contact details of the controller;

b. **the personal data being processed as such**;

c. the **purpose of processing**;

d. the **period of storage** of the personal data or, if this is not possible, the criteria used to determine such period;

e. the available information on the **origin of the personal data**, to the extent that it was not collected from the data subject;

f. if applicable, **the existence of an automated individual decision as well as the logic on which this decision is based**;

g. if applicable, **the recipients or categories of recipients** to which the personal data was disclosed as well as the information foreseen in Article 19 paragraph 4.

Access Right – Art. 25 DSG (2)

3 Personal data on the data subject's health may be communicated to the data subject, provided his consent is given, by a healthcare professional designated by him.

4 **If the controller has personal data processed by a processor, the controller remains under the obligation to provide information**.

5 **No one may waive the right to information in advance**.

6 The controller provides the requested information **free of charge**. The Federal Council may provide for exceptions where information shall not be provided free of charge, in particular if the effort involved is disproportionate.

7 **As a rule, the information shall be provided within 30 days**.

Limitations to the Access Right – Art. 26 DSG

- several reasons give the controller the right to refuse, restrict or defer provision of information - i.e.
  „c. the request for information **is manifestly unfounded in particular if it pursues a purpose that is contrary to data protection or is obviously of a frivolous nature.**“
  or
  „2 Additionally, it is possible to refuse, restrict or defer the provision of information in the following cases:
  a. when the controller is a private person and the following conditions are fulfilled:
  1. **if prevailing interests of the controller require the measure**.
  2. **the controller does not disclose the personal data to a third parties**.

Right of Data Portability – Art. 28 DSG

1 **Any person may request from the controller, free of charge, the disclosure of the personal data that he has disclosed to him in a standard electronic format if:**

a. the controller processes the data **in an automated manner**; and

b. t**he data is processed with the consent of the data subject** or in direct connection with the conclusion or performance of a contract between the controller and the data subject.

2 In addition, the data subject **may request the controller to transfer his personal data to another controller** if the requirements in accordance with paragraph 1 are met and this does not involve a disproportionate effort.

3 The Federal Council may provide for exceptions to this freedom of charge, in particular if the effort involved is disproportionate.

Sanctions

On complaint, private persons are liable to a fine of up to **250'000.–** Swiss Francs if they wilfully do not...

- ...provide access and information or to cooperate - Art. 60 revDSG
- ...violate the duties of diligence - Art. 61 revDSG
- ...breach the professional confidentiality - Art. 62 revDSG
- ...disregard decisions - Art. 63 revDSG
- ...violate committed within undertakings - Art. 64 revDSG (exception)

Employment & Data Protection – Art. 328b OR

„The employer may data about the employee **only** process as it concerns **his qualification for the employment** or are **inevitable for the execution of the employment**. The regulations of the Swiss Data Protection Act are applicable.“

EU-law is applicable for Swiss Companies (GDPR)

- **EU-GDPR** (General Data Protection Regulation - DSGVO)
- **Directly applicable for all Swiss Companies if they address to customers in the EU (by using € or language) and are collecting personal data! (i.e. when using Google-Analytics!)**
- Stronger requirements i.e. in informing the data subjects about the reason, the categories, the recipients and the rights they have when a company collects personal data.
- A responsive has to be named in the public
- Has to be organised since **May 25th, 2018**!
- Draconic fines (up to 20 Mio. €)! www.enforcementtracker.com

Simple Case

Nova-AG, headquartered in Dornbirn (AT), has developed a software (mobile app) that enables large companies to collect automatically the tour/visits of their sales representatives. The Sales Managers automatically receive work profiles of their employees through the system and can thus control the effectivity of their sales reps.

Nova AG has a subsidiary in Switzerland, which sells the software and the service that is hosted by AWS (Amazon Web Service) in the U.S.

What is the data protection situation?

My Take Away?

- ...
- ...
- ...
- ...
- ...