NIEDERER KRAFT FREY

Swiss Data Protection Law

Partner Compliance Practice

Zurich — 20 April 2021

Table of Contents

- ✓ Overview on which law applies and which authorities are in charge
- ✓ Give you a basic understanding of the principles of Swiss Data Protection Law
- ✓ Give you insights on cross-border data transfer
- ✓ Discuss some topics around personal data in the Cloud
- ✓ Give you some insights on the principles of GDPR
- ✓ Overview on the new Swiss Data Protection Law

General

Legislation and Authorities

What is the principal data protection legislation?

- Federal Act on Data Protection as of 19 June 1992 (FADP)
- The FADP has been revised and will come into force in 2022

Is there any other general legislation that impacts data protection?

- Each Swiss Canton has its own data protection laws with respect to data processing of Cantonal public authorities

Is there any sector specific legislation that impacts data protection?

- Banks: when bank customer data are processed
- Health: when patient data are processed
- Secrecy obligations: when public authorities, lawyers, etc. process client data

What is the relevant data protection regulatory authority?

- Federal Data Protection and Information Officer (FDPIC) when personal data are processed by federal authorities, individuals and legal entities
- Cantonal Data Protection and Information Officer when personal data are processed by public authorities of the respective Canton

What is Data Protection?

- It is not about protecting the data, but the personality rights of the data subjects who own such data
- Data subjects have important rights, including the right to find out what personal information is held about them
- Anyone who processes personal information must comply with the data protection principles

Personal Data and Sensitive Personal Data

What is personal data?

So, what is sensitive personal data?

Personal Data

- **Personal Data:** any piece of information through which a person can be, directly or indirectly, identified
- **Examples** of personal data: name and surname; home address; email address; identification card number / social security number, etc.
- Microsoft data **processing examples**:
  - staff management and payroll administration
  - access to a contacts database containing personal data
  - sending promotional emails
  - shredding documents containing personal data
  - posting/putting a photo of a person on a website
  - storing IP addresses or MAC addresses
  - video recording (CCTV)

Sensitive Personal Data

As defined in the Swiss FADP and GDPR:

- **racial or ethnic** origin
- **political** opinions,
- **religious beliefs** or other beliefs of a similar nature,
- membership of a **trade union**
- **physical or mental health** or condition,
- **sexual** life,
- the commission, or alleged commission, of **any offence**, or
- any **court proceedings** or sentence relating to any offence committed or alleged to have been committed.

FADP Terminology I

- **Consent:** explicitly and freely given, specific and informed. It has to be given by statement and to be proven. Data subjects can withdraw consent at their discretion
- **Data Subject:** any individual whose personal data is being processed
- **Data Controller:** any company or organization that collects individual's personal data and determines how to process these data

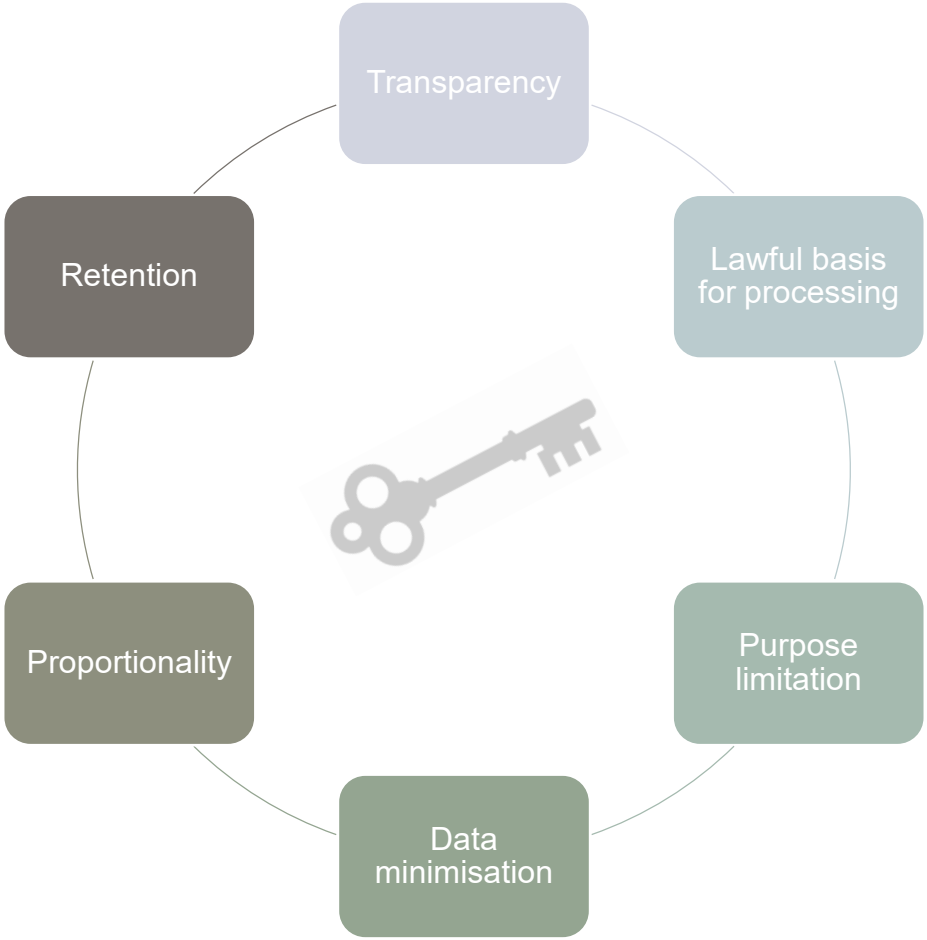
FADP Terminology II

- **Data Processor:** any company or organization that processes the data on the behalf of Microsoft but does not decide what to do with the handled data
- **FDPIC:** the Swiss Federal Data Protection and Information Commissioner which is the Swiss supervisory authority
- **Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use

FADP Terminology III

- **Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction or access to personal data. A personal data breach can include access by an unauthorized third party, deliberate or accidental action by controllers or processors, alteration of personal data without permission and loss of availability of personal data
- **Third Countries:** any country outside the EU borders which does not have an equivalent data protection level like Switzerland or the EU

Key principles for the processing of personal data



Transparency

Items of information to be provided:

- Identity, data uses and legal basis
- Legitimate interests pursued
- Recipients or categories of recipients of data
- Cross-border dataflows and safeguards
- Data storage period
- All available rights

The Role of Consent

- Decide when consent is needed
- Valid consent will be much harder to achieve under FADP
  - consent must be specific, informed and freely given
  - consent cannot be bundled with T&Cs
  - consent can be withdrawn at any time and in an easy way
  - if "take it or leave it" not freely given
- Consent does not remove the need to comply with the other principles

Individual Rights

- Access to data
- Correction and deletion or requesting the erasure of personal data held by an entity
- Objection to processing
- Objection to marketing
- Complaint to relevant data protection authority
- Find out why an organisation holds personal data
- Find out to whom an organisation has disclosed personal data
- Know the source of the personal data held
- Transfer a copy of personal data to another party, known as the "right to data portability"

Registration Formalities and Data Protection Officer

In what circumstances is it required?

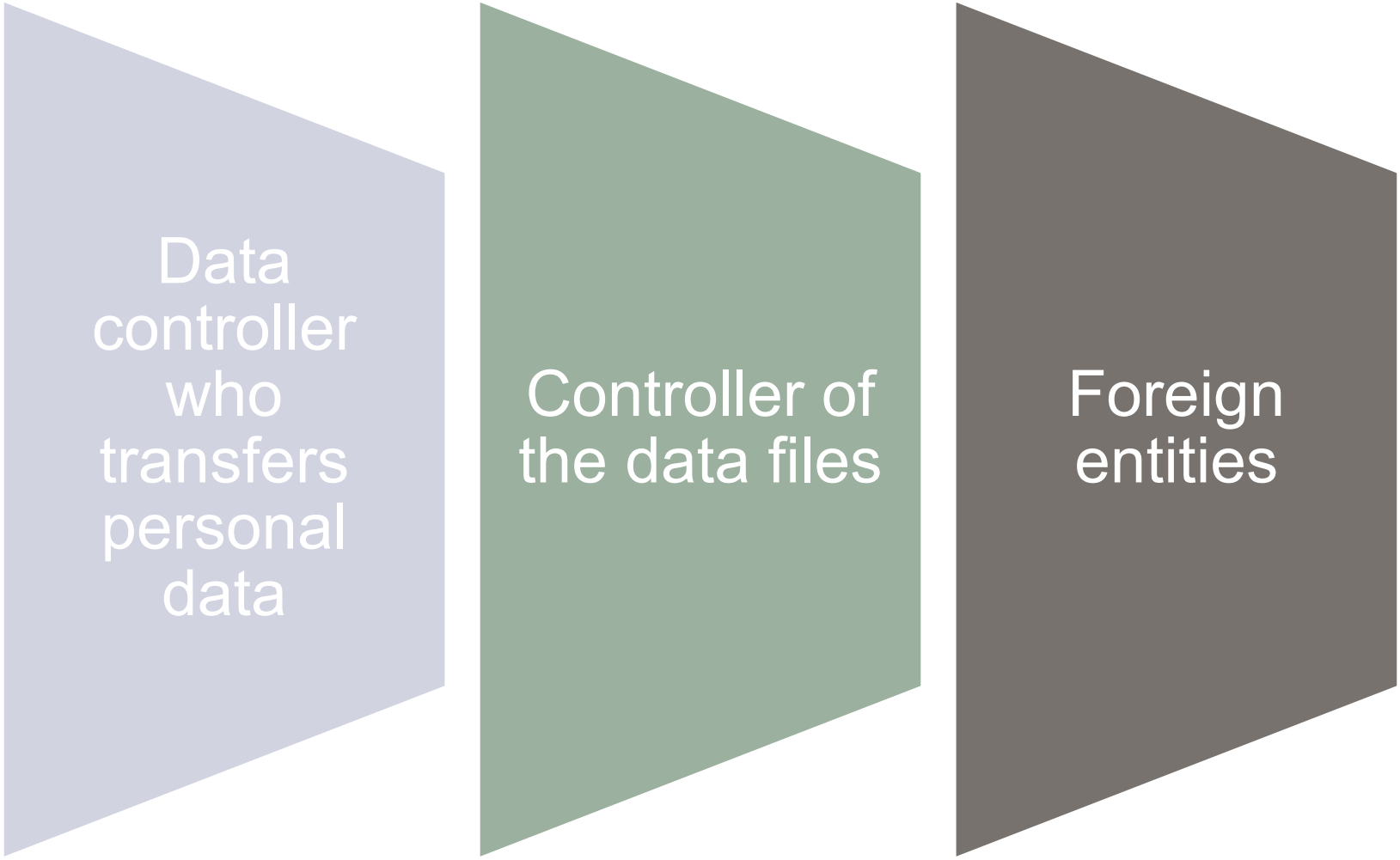
Cross-Border Data Transfer

- To a country that has no appropriate data protecting laws in force, additional safeguards are necessary
- Safeguards: i.e. data transfer agreements or group-wide data protection policies
- FDPIC must be informed about these safeguards
- If standard contractual clauses of the EU or the FDPIC are used, sufficient to inform the FDPIC about it in a general way

Data Files with the FDPIC

- Federal Bodies must register their data files with the FDPIC in any case
- Private persons must register their data files with the FDPIC only if they:
  - regularly process sensitive personal data/personality profiles
  - regularly disclose personal data to third parties

Who must register?



Register Information

What information must be included in the registration/ notification?	– **Cross-border transfer**: no detailed information required, if standard contracual clauses of the EU/FDPIC are used – **Registration of data files**: notifying entity, contact person, categories of personal data, data subjects, data recipients, persons having access to data files
Sanctions for failure to register/notify?	– Entities or individuals may be fined with up to CHF 10,000
What is the fee per registration?	– No fee for the registration of data files
How frequently must registrations/notifications be Renewed?	– As soon as the notified information changes – No strict deadline
For what types of processing activities is prior approval required?	– There is no such obligation. Regarding federal and cantonal – authorities, such approval obligations may arise out of special – public regulation

Appointment of a Data Protection Officer

Advantages: Data files must not be registered with FDPIC anymore

Specific qualifications: Independence

No sanctions for failing to appoint a DPO

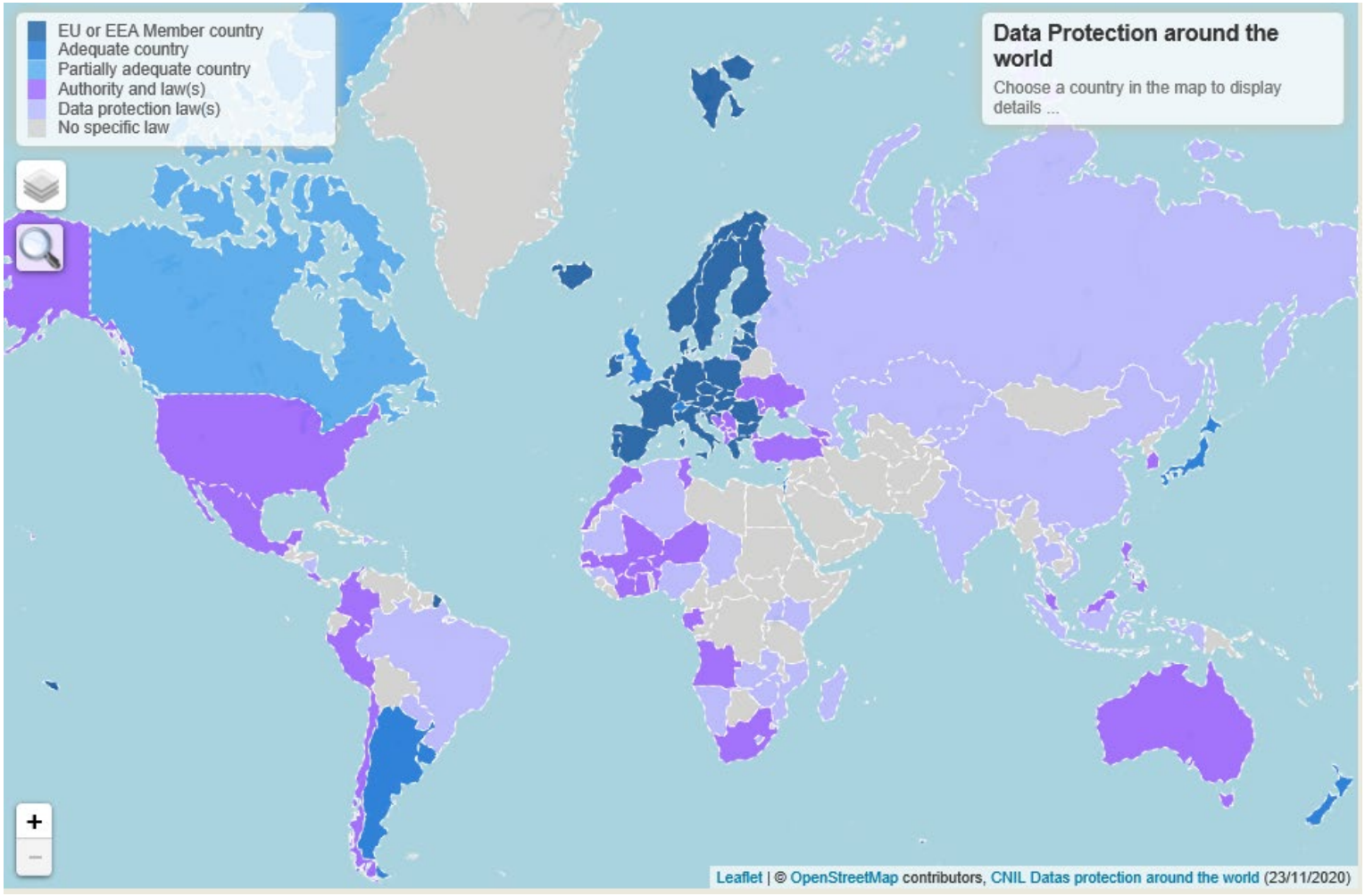
DPO must be registered/notified to the relevant authorities

Responsibilities:
- Monitoring the processing of personal data and suggesting correction measures
- maintaining a list of all data files

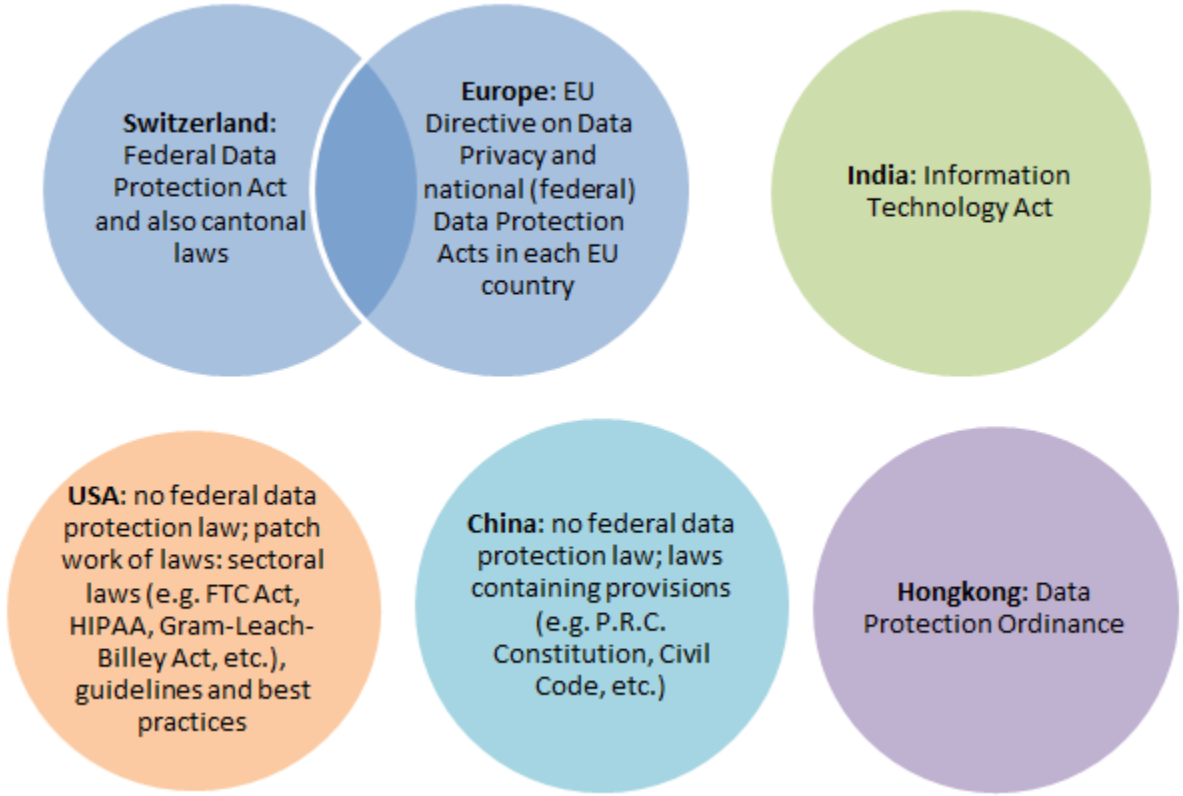
Appointment of DPO is optional

Restrictions on International Data Transfers

Countries with adequate Data Protection Laws



Different Data Protection Regimes World-Wide



Restrictions I

- No cross-border transfers to countries that do not ensure an adequate
- See list of countries without adequate data protection level: […]
- Transfer of personal data abroad means: any provision of personal data abroad, including allowing **access**, **examination**, **transfer** or **publication**

Restrictions II

FDPIC allows transfers to such countries, when

- sufficient contractual guarantees are implemented with the recipient: e.g. EU Standard Contractual Clauses
- the data subject consented to the specific transfer.
- the conclusion or performance of this contract requires transfer of the contracting party's personal data
- there is an overriding public interest
- the transfer is necessary to enforce legal rights before a court.
- the data subject made the personal data generally accessible and has not objected to its processing

Data in the Cloud

Processing Data in the Cloud

- Permitted to process personal data in the cloud
- A **written** data processing agreement between data controller and cloud provider is needed
- The agreement must include **instruction**, **monitoring** and **audit rights** on behalf of data controller
- Right to obtain information and right to have data deleted/corrected **must be respected**

Using a Cloud Provider (Outsourcing)

- Conclude written contract with following items:
  - Individuals processing data must be committed to confidentiality
  - Must flow down obligations to sub-processors
  - Support the controller in breach notifications to DPAs/data subjects
  - Delete or return all personal data at the end of provision of services
  - Provide information to controller to demonstrate compliance
  - Allow for and contribute to audits
- Technical and organisational measures (TOMs): service provider must apply TOMs to protect Microsoft personal data

Data Security

Data Security

Data need to be protected from:

- Unauthorised or accidental destruction
- Accidental loss
- Technical faults
- Forgery, theft, unlawful use
- Unauthorised alteration, copying, acccess or other unauthorised processing

Sanctions

Sanctions

Civil law	Public law	Criminal law
• Art. 15, Swiss FADP and Art. 28 et seq.	• Art. 29(1), Swiss FADP	• Art. 34 and 35, Swiss FADP

GDPR

Legal Framework

EU General Data Protection Regulation

- Directly applicable
- 25 May 2016: Entry into force
- 25 May 2018: Applicability

National laws

- Opening clauses in GDPR
- Germany, Ireland, Netherlands, etc.

The Aim behind GDPR (II)

- **Extraterritorial** reach
- Putting people in **control**
- Focus on **pratical** compliance
- Stronger **enforcement** powers

GDPR applicable to Microsoft?

- **Yes!**
- Applicability to all Microsoft companies based **in EU** countries
- **Outside the EU** applicability based
  - on **establishment** or economic activity in EU Member State (cross-border)
  - on **individuals being** in the EU
    - offering of goods or services to them (e.g. website access)
    - monitoring of their behaviour (e.g. cookies when visiting website)
  - Generally speaking: applicability based on the fact that Microsoft is processing **personal data coming from the EU** in its non-EU territory

Revision of FADP

Revision of the Swiss Data Protection Act (DPA)

- Current Data Protection Act is from 1992
- Technological developments and the GDPR necessitated the revision
- Parliamentary adoption in autumn 2020
- No referendum was requested
- Administration is currently drafting the corresponding ordinances
- Important take-aways:
  - No copy of the GDPR: high degree of abstraction and technology-neutral
  - Renewal of EU's recognition of data protection equivalence expected in 2021
  - No general transition period: **be ready & compliant by 2022**

Overview of most important revisions I

- DPA no longer applicable to personal data of legal entities (Art. 1)
- DPA applicable if effects in Switzerland, even if processing takes place abroad (Art. 3)
- Terminology adopted: "profiling with high risk", "data security breach", "controller", "processor" (Art. 5)
- New concept of "privacy by design" and "privacy by default" (Art. 7)
- TOMs to avoid data security breaches (Art. 8)
- Voluntary appointment of DPO **[*Datenschutzberater*]** (Art. 10)
- Codes of conduct (Art. 11)
- Records of processing activities (Art. 12)
- Certification (Art. 13)
- Representative (Art. 14)

Overview of most important revisions II

- Information to be given upon collection of personal data (Art. 19-21)
- Data protection impact assessment (Art. 22, 23)
- Notification of data security breach (Art. 24)
- Right of access (Art. 25, 26)
- Data portability (Art. 28)
- Investigations (Art. 49)
- Competences of FDPIC (investigations Art. 50, measures Art. 51)
- Criminal sanctions (Art. 60-64)
- Competence for criminal sanctions (Art. 65)

Hot Topics and Questions

Hot topics

- Big Data
- Data tracking by apps (e.g. fitness apps)
- Data protection and personalised healthcare
- Data protection and drones used by individuals for private purposes
- Dashcams (small video recorders often used in cars)
- Right to be forgotten
- Cloud Computing

THANK YOU

Questions?

THANK YOU

Your Contact

Clara-Ann Gordon

clara-ann.gordon@nkf.ch

D +41 58 800 84 26

Niederer Kraft Frey Ltd Bahnhofstrasse 53 CH-8001 Zurich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch