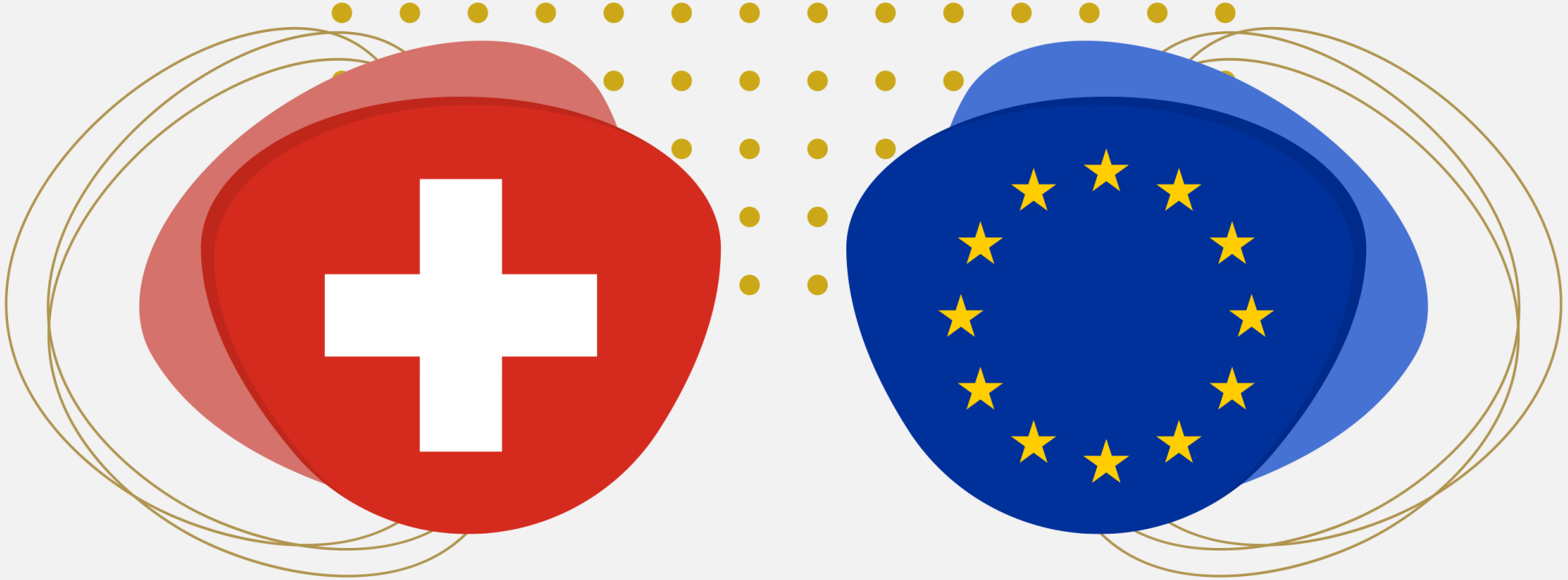


The new Swiss Data Protection Act - What you need to know

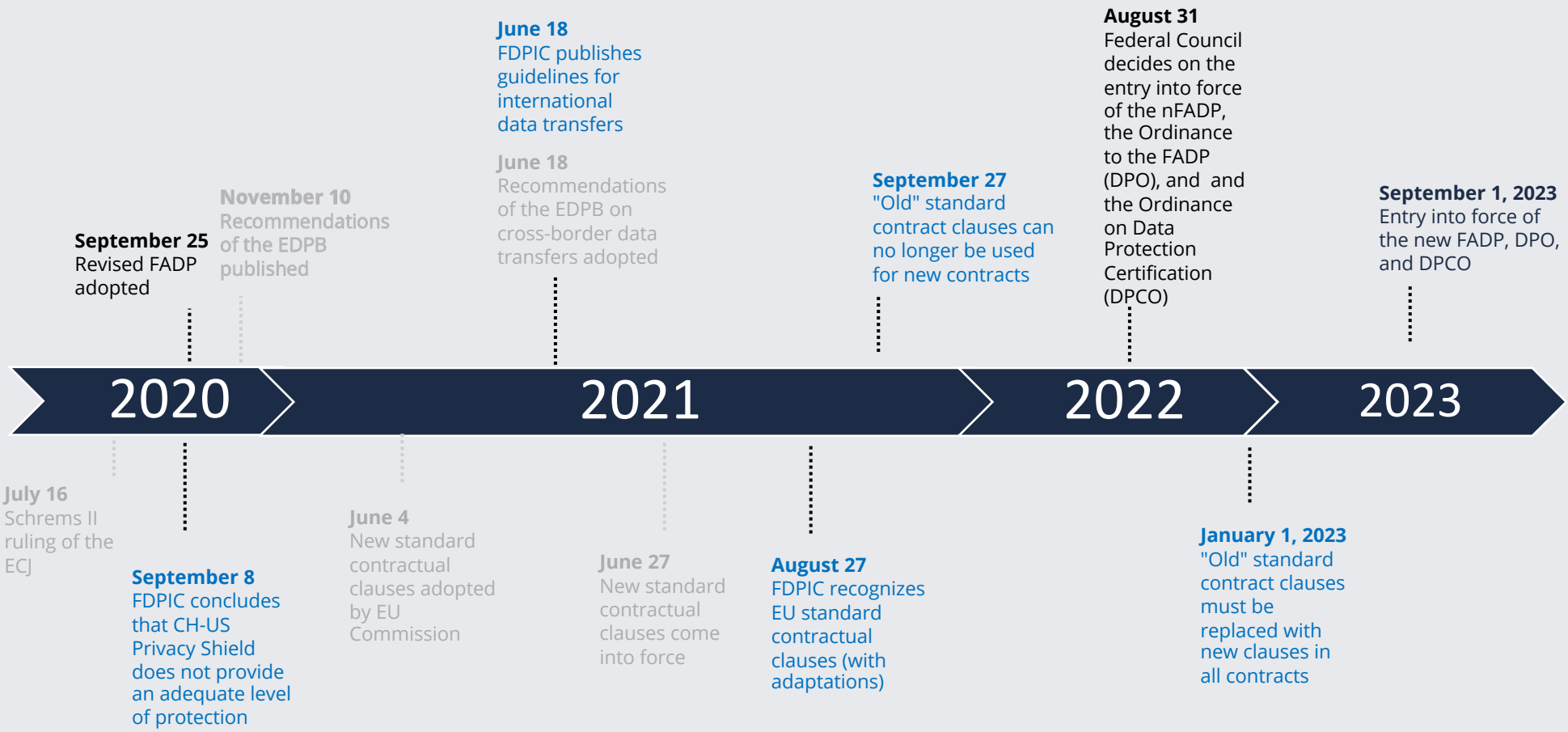
Daniela Fábián Masoch, FABIAN PRIVACY LEGAL

Mondaq, 7 December 2022

FABIAN
PRIVACY
LEGAL

Table of Contents

Developments in Switzerland



Revision of the Swiss Federal Data Protection Act (nFADP)

The Federal Data Protection Act (FADP)

- was revised with the main objective to achieve the alignment of the Swiss Data Protection Act with EU law and the Council of Europe Convention on Data Protection (Convention 108);
- was adopted on September 25, 2020, and enters into force with the Ordinance to the FADP (DPO), and the Ordinance on Data Protection Certification (DPCO) on **1 September 2023** (with no transitional period);
- regulates data processing by private persons (companies) and federal bodies as before;
- adopts many regulations of the GDPR, but remains more pragmatic overall;
- remains principle-based, as before, and is less detailed than the GDPR;
- retains the basic concept of «permission subject to prohibition» (contrary to the GDPR: prohibition subject to permission);
- only applies to the processing of personal data of natural persons and applies to all actions that have an impact in Switzerland, even if they are carried out abroad (impact principle).

What applies according to the current FADP?

- **Scope**: personal data = all information relating to an identified or identifiable natural or legal person (new: natural persons only)
- **Data protection principles** (lawfulness; good faith; transparency; purpose limitation; proportionality; accuracy; however, no accountability principle)
- **Data subject rights** (information, access, rectification, deletion, restriction of processing, right to object - new: right to data portability)
- **Data security**
- **Register of data files / registration with the FDPIC** (new: record of processing activities / registration no longer required for private persons)
- Due diligence and contract for **outsourcing** of data processing
- Rules for **cross-border transfers**, especially to countries without an adequate level of protection; information to the FDPIC

What is newly regulated?

Territorial and material scope *Impact principle / natural persons*	Definitions *i.e., processor, controller, sensitive personal data, data security breach*	Extended duty of information (including automated decisions)	Obligation to delete / anonymize
Data portability	Privacy by Design/Privacy by Default	DPIA	Data protection advisor
Record of processing activities	No sub-processing without prior authorisation	Cross-border data transfer *Federal Council determines adequate countries*	Risk-based approach for data security
Notification of data security breaches	Representative in Switzerland	Administrative measures	Penal provisions

Where does the nFADP differ from the GDPR?

Basic concept

Permission subject to prohibition

Scope

Impact principle */ manual processing*

No accountability principle

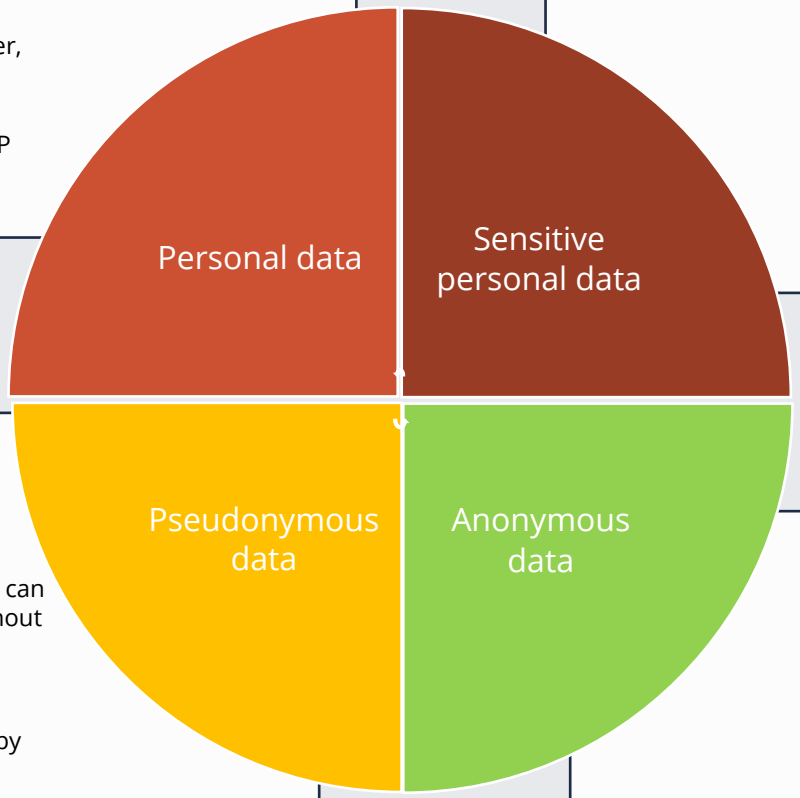
Notification of data security breaches is more pragmatic

Duty of information includes third countries in case of cross-border data transfers; more exceptions

Penal provisions

What is personal data under the nFADP?

Person is identified or identifiable by
- Identifier (e-mail, name, photo)
- Identification number (passport number, personal social security number, code)
- Location data
- Online identification (e.g. cookies and IP address)
- Combination of factors



- Data on religious, ideological, political or trade union related views or activities
- Data on health, the intimate sphere or the racial or ethnic origin
- Genetic data
- Biometric data that uniquely identifies a natural person
- Data on administrative and criminal proceedings and sanctions
- Data on social security measures

- Term not defined in the FADP
- According to GDPR: personal data that can no longer be assigned to a person without additional information / additional information is stored separately and secured
- In practice: replacement of identifiers by numbers
- Switzerland: relative approach

- Term not defined in the FADP
- Removal of all direct and indirect identifiers from personal data - identification no longer possible
- Anonymized data is not personal data!

Data protection principles

Lawfulness / good faith	•Personal data must be processed lawfully and in good faith
Proportionality	•Data processing must be proportionate (data must be necessary, adequate and appropriate for the purpose - data minimization)
Purpose limitation	•Personal data may only be collected for a specific purpose which is evident to the the data subject; it may only be processed in a way that is compatible with this purpose. (Attention: Purpose description in the privacy notice should include all purposes and disclosure to third parties! If not, a legal justification (e.g., consent) is required for subsequent changes of purpose
Storage limitation	•As soon as personal data is no longer required to fulfil the purpose (or the purpose has been fulfilled), the personal data is destroyed (deleted) or anonymized

Data protection principles

Data accuracy	•Anyone who processes personal data must ascertain that the data is accurate and take all appropriate measures (taking a risk-based approach) to ensure that inaccurate or incomplete data is corrected, deleted or destroyed if necessary
Data security	•Personal data must be protected against unauthorized processing trough adequate technical and organizational measures that enable the avoidance of data security breaches – the minimum requirements are regulated in the Ordinance (DPO)
Will of the person concerned	•Personal data may not be processed against the express declaration of intent without justification (consent, overriding private or public interest, or law)
Disclosure to third parties	•Sensitive personal data (under the current law also personality profiles) may not be disclosed to third parties without justification

Anyone who violates data protection principles must have a justification

- Anyone who processes personal data in contravention with the data protection principles, violates the personality of the data subject (the data subject may bring an action against the data processor in civil court).

- However, no violation of the personality if
  - The data subject has made the personal data generally accessible and has not expressly prohibited ist processing
  - There is a justification
    - Consent of the data subject
    - Overriding private or public interest (e.g., processing the data of the contractual partner for the conclusion or execution of a contract)
    - Law

Profiling and high-risk profiling

Profiling

- «Any type of **automated processing** of personal data that consists of using such data to **evaluate certain personal aspects** relating to a natural person, in particular to **analyze or predict** aspects relating to that natural person's job performance, economic situation, health, personal preferences, interests, reliability, behavior, location or change of location»
- **In short**: automated processing - aims to evaluate (analyze, predict) certain personal aspects (personalized advertising, financial analysis, performance review)
- **Consequences**: None

High risk profiling

- Profiling which involves a high risk to the personality or fundamental rights of the data subject, by leading to the **linking of data** allowing **an assessment of essential aspects of the personality of** a natural person
- **In short**: automated processing that leads to the linking of data - aims to assess essential aspects of the personality
- **Consequences**:
  - DPIA
  - Protocol (log of storage, modification, reading, disclosure, deletion and destruction of the data)
  - Processing regulation/rules (internal organization, controls, data security measures)
  - If consent is required, it must be explicit

Duties of the controller (and processor*)

Duty to inform	Duties based on data subject rights (access, data portability, correction and deletion)	Data processing by processors*	Cross-border transfer of personal data*
Privacy by Design / Privacy by Default	Data security* Data security breach notification (Processor notifies controller)	Record of processing activities*	Data protection impact assessment

Duty to inform

- The controller shall adequately inform data subjects about the direct or indirect collection of personal data (so far only for sensitive data and personality profiles) – The DPO contains the modalities.

Minimum content

- Controller's identity and contact information
- Purpose of processing
- If applicable, recipients or categories of recipients to whom personal data is disclosed
- Categories of personal data (if collected indirectly)
- For cross-border data transfers, the state and applicable transfer mechanism/exception
- If applicable, automated individual decision - decision based exclusively on automated processing which has legal effects on the data subject or affects him/her significantly

Exceptions and restrictions

- No information if
  - Data subject already has the information
  - Processing is provided for by law
  - The controller is bound by a legal obligation to secrecy
  - With indirect collection, where information is not possible or requires a disproportionate effort
- Limitation, deferral, or waiver if, for example,
  - The measure is required by overriding interests of third parties
  - The information prevents the fulfilment of the purpose of the processing or
  - The controller has overriding interests and does not disclose the data to third parties (companies controlled by same legal entity are not considered third parties)

Time of information

- Direct collection: at the time of collection
- Indirect collection: no later than one month after receipt of the data or earlier if data is disclosed (time of disclosure)

Duty to inform in the case of an automated individual decision

Definition

- Individual decision
  - is based exclusively on automated processing (both the assessment of the facts and the decision - no influence by a natural person / no if-then decisions) that has
  - legal consequences for the data subject or significantly affects him or her

Duties and rights

- The controller informs the data subject of an automated individual decision
- The data subject may request to state his or her position (and ask how the decision was reached) and may request that a natural person review the automated individual decision

Exceptions

- No information obligation and rights if
  - the decision is directly related to the conclusion or performance of a contract between the controller and the data subject and the data subject's request is granted, or
  - the data subject has expressly consented to the decision being automated

Record of processing activities

- **Controllers (and processors) must keep a record of their processing activities. Notification to the FDPIC no longer necessary, except for federal bodies.**
- **The record contains at least the following:**
  - Controller's identity
  - Purpose of processing
  - Description of the categories of data subjects and personal data processed
  - Categories of recipients
  - Retention period or criteria for determining this period
  - General description of the data security measures
  - In case of cross-border disclosure, indication of the state and the safeguards
- **Exemptions for companies when:**
  - < 250 employees and
  - data processing is associated with a low risk for the data subjects (according to the DPO: no extensive processing of sensitive personal data, no high-risk profiling)

Data security - Technical and organizational measures (TOMs)

- The controller and the processor shall ensure data security appropriate to the risk by means of suitable technical and organizational measures (TOMs). The TOMs should prevent data security breaches.
- The DPO contains the criteria for determining appropriateness and protection goals (no specific minimum TOMs).
- The controller and the processor are responsible to determine and implement the appropriate security measures based on the criteria.
- For automated processing of sensitve data on a large scale or high-risk profiling, the data controller and the processor must keep a log and create processing regulations.

Security principles and goals

To ensure adequate data security, the controller and processor must
determine the protection needs of the personal data, and
determine the appropriate technical and organizational measures (TOM) according to the risk.

determine the protection needs of the personal data

- **Criteria for assessing the need for protection**
  - the types of data, and
  - the purpose, nature, scope and circumstances of the processing

determine the appropriate technical and organizational measures (TOM) according to the risk.

- **Criteria for determining the risk**
  - Causes of the risk
  - Main hazards
  - Measures taken or envisaged to mitigate the risk
  - Probability and severity of data breach despite measures taken or envisaged
- **Criteria for determining the TOMs**
  - State of the art, and implementation costs, with the goal to ensure confidentiality, availability, integrity, and traceability (specifications in the DPO)

Data security breach

Data security breach: A breach of security (confidentiality, integrity or availability) that results in personal data being inadvertently or unlawfully lost, deleted, destroyed or altered, or disclosed or made accessible to unauthorized persons.

Who must notify whom within what timeframe	• The controller shall report the breach to the FDPIC as soon as possible and inform the data subjects (GDPR - within 72 hours of becoming aware of it). • The processor shall notify the breach to the controller as soon as possible (GDPR - without undue delay)
When to notify and inform	• Notification to FDPIC if breach is likely to result in a high risk to the personality or fundamental rights of the data subject (evaluation on a case-by-case basis!) (GDPR - risk) • Information of the data subject if it is necessary for his or her protection (the data subject can do something to minimize the risk or mitigate the consequences) or if the FDPIC requests it (exceptions according to Art. 24 para. 5 nFADP, e.g., if the information is impossible or requires a disproportionate effort or information is provided by public notice) (GDPR - high risk).
What must the notification to the FDPIC contain	• Nature of the data security breach, its consequences and the measures taken or envisaged

Data protection impact assessment (DPIA)

When to conduct a DPIA

- The controller shall conduct a DPIA if a planned data processing operation may entail a high risk to the personality or fundamental rights of the data subject.

- The high risk arises in particular
  - When using new technologies (e.g., use of AI).
  - From the type, scope, circumstances and purpose of the processing, e.g.
    - for automated individual decisions
    - for high-risk profiling
    - in the case of extensive processing of sensitive personal data
    - when extensive public areas are systematically monitored

- Possible impacts of the processing on the data subject are
  - Inability to exercise rights or access certain services or opportunities
  - Loss of control over the use of personal data; the loss of confidentiality
  - Discrimination, identity theft or fraud
  - Financial loss, reputational or physical damage
  - Re-identification of pseudonymized data

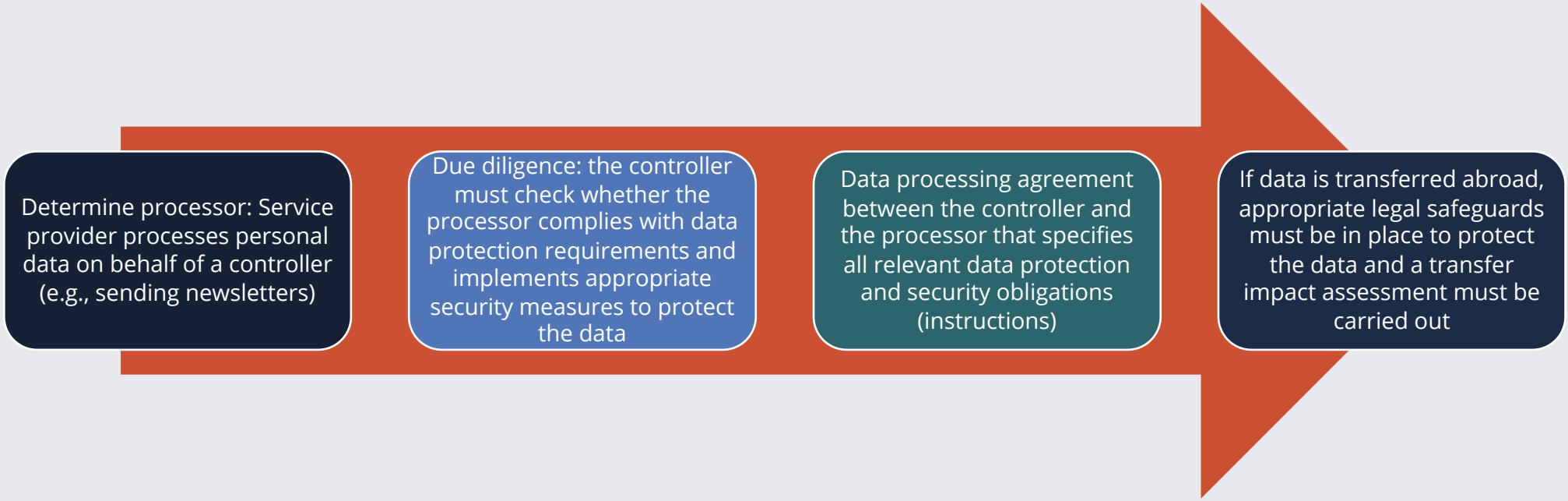
Data protection impact assessment (DPIA)

How to conduct a DPIA

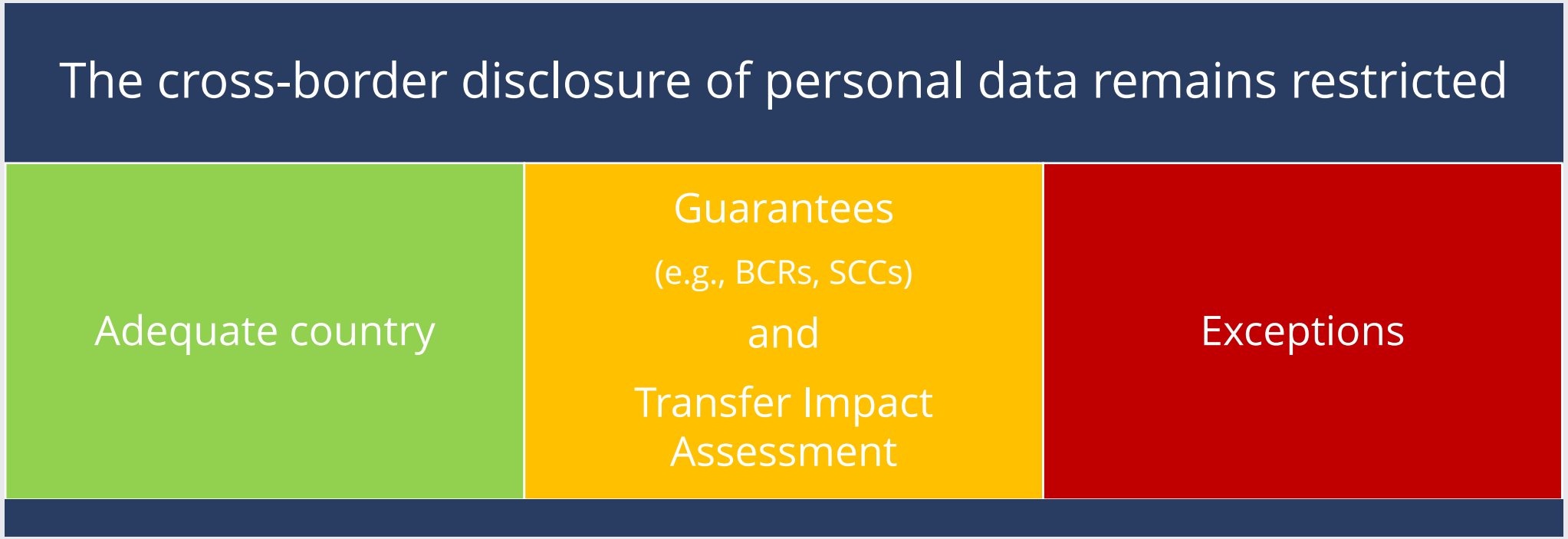
- A DPIA is a **process** that helps the data controller assess the risks of a planned data processing operation and determine measures to mitigate those risks. The DPIA contains:
  - a description of the planned data processing,
  - an assessment of the risks to the personality or fundamental rights of the data subject, and
  - the measures taken to protect personality or fundamental rights.
- The controller performs the DPIA **before** data processing
- **Consultation of FDPIC** in case of high risk despite measures taken (exception: consultation of appointed data protection advisor)
- **Exceptions** for private controllers:
  - Controller is legally obliged to process data
  - Controller is subject to a code of conduct that meets the legal requirements

Outsourcing

- The controller may assign by contract or by legislation the processing of personal data to a processor if
  - the data is processed in the same way as the controller would be permitted to do himself, and
  - no legal or contractual confidentiality obligation prohibits the assignment.
- The controller must ensure that the processor is able to guarantee security.
- NEW: The processor may only transfer the processing to a third party with the prior approval of the controller



Cross-border disclosure of personal data



The data protection advisor

- Controll can appoint a data protection advisor.

- Tasks
  - Point of contact for data subjects and authorities,
  - Training and advising the controller on data protection issues,
  - Assistance in the implementation of the FADP

- Requirements for benefitting from the exemption to consult the FDPIC for high-risk processing
  - Professional independency and no instructions
  - No conflict of interest
  - Required professional knowledge
  - The contact details of the data protection advisor are published and the FDPIC is notified

Privacy by design / privacy by default

- New obligation - best practice
- Is the basic condition for the effective implementation of data protection
- ensures compliance with legal requirements and principles and enables strategic and operational decisions to be made at an early stage in order to design business processes and systems efficiently

Privacy by design	•The controller must, from the outset, design the data processing technically and organizationally in such a way that the data protection requirements and principles are complied with •The TOMs must be appropriate (i.e., corresponding to the state of the art, the type and scope of processing, and the risks that the data processing entails for the personality and rights of the data subjects)
Privacy by default	•The controller implements appropriate pre-defined settings to ensure data minimization •Data subject may decide differently

Sanctions (Art. 60ff. nDSG)

- On complaint, private persons (individuals) are punished by a fine of up to 250,000 Swiss Francs if they
  - violate their obligations by intentionally providing false or incomplete information (art. 19, 20, 25-27)
  - intentionally fail
    - to inform the data subject in accordance with art. 19.1 and 21.1, or
    - to provide him or her with information in accordance with Art. 19 Para. 2 FADP
  - intentionally disclose personal data abroad in violation of Art. 16 and 17 FADP
  - intentionally assign data processing to a processor without meeting the conditions of Art. 9.1 and 2 (prerequisites for processing, due diligence)
  - intentionally fail to comply with the minimum data security requirements (Data Protection Ordinance)
  - intentionally disclose secret personal data of which they have gained knowledge while exercising their profession which requires knowledge of such data
- Private persons (individuals) are liable to a fine up to 250‘000 Swiss Francs if they intentionally provide false information to the FDPIC in the course of an investigation or intentionally refuse to cooperate

Art. 8.3	Minimum requirements for data security (according to DPO)
Art. 9.1, 2:	Requirements for assigning a data processor, due diligence
Art. 16.1., 2:	Cross-border principle and guarantees
Art. 17:	Cross-border derogations
Art. 19, 20:	Duty to inform when collecting personal data, and exceptions
Art. 21:	Duty to inform in the case of automated individual decision
Art. 25-27:	Duty to provide information upon request (access right)

Recommendations for implementation

- Conduct a **data management and compliance analysis** to identify potential gaps, risks, and required actions.
- Implement a privacy by design process and **processes** to ensure deletion and destruction of personal data and support data portability.
- Review your **privacy statements** and amend them as necessary.
- Create a **record of processing activities** and implement a process to conduct **compliance audits** and **data protection impact assessments**.
- Review your **relationships with vendors and associated data flows** and take appropriate action (taking into account the latest developments and FDPIC policy documents, i.e., vendor assessments, TIAs, SCCs),
- Review your **data security safeguards**; conduct assessments to determine the level of protection, and implement risk-appropriate technical and organizational measures
- Implement appropriate processes and responsibilities for **handling data breach notifications** and **requests for information from data subjects**
- Review your **organizational structure** for handling data protection, assess if you need to appoint a **Data Protection Advisor**
- Review, and, if necessary, amend or create new **internal standards and processes** to ensure compliance with data protection requirements.

Questions?

Daniela Fábián Masoch
FABIAN PRIVACY LEGAL GmbH
www.privacylegal.ch

daniela.fabian@privacylegal.ch