



# Get ready for the new Swiss Data Protection Act

Daniela Fábíán Masoch, FABIAN PRIVACY LEGAL

Mondaq, 8 June 2023

# Introduction

- This webinar builds on the previous presentation of 7 December 2022

## **The new Swiss Data Protection Act – What you need to know**

- The focus is on the implementation of the new Swiss Data Protection Act (FADP) and its ordinance (DPO) by private companies (not federal bodies)



# Applicability of the FADP

## Requirement – Impact principle

The FADP applies to matters that have an impact in Switzerland, even if they are initiated abroad.

## To do – Assess if the new FADP applies to your organization

- ✓ The organization has its registered office in Switzerland
- ✓ Processing takes place in Switzerland
- ✓ Natural persons affected by the data processing (data subjects) have their usual place of residence in Switzerland
- ✗ None of the requirements are met

# Appointment of a representative in Switzerland

**Requirement** – Private controllers located abroad must designate a representative in Switzerland to act as contact point for the FDPIC and data subjects if all the following conditions are met:

- the organization processes personal data of persons in Switzerland, and
- the data processing is connected to
  - offering goods or services in Switzerland or
  - monitoring the behavior of these persons, and
- the processing is extensive, and
- it is a regular processing, and
- the processing involves a high risk for the personality of the data subjects.

# Appointment of a representative in Switzerland – to do

**To do** - Assess whether a representative must be appointed in Switzerland

- ✅ Appoint the representative in writing (recommendation), and specify the duties:
    - to keep a register of the processing activities (minimum content in Art. 12.2 FADP),
    - on request, to provide the FDPIC with the information contained in the register,
    - on request, to provide the data subjects with information on how to exercise their privacy rights
- Publish the name and the address of the representative (e.g., in the privacy notice)

# Appointment of a data protection advisor

**Requirements** – the controller may appoint a data protection advisor (not mandatory):

## **Tasks of the advisor:**

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

**Benefit:** Exemption to consult with the FDPIC for high-risk processing, under the conditions:

- Professional independency and no instructions
- No conflict of interest
- Necessary professional knowledge
- The contact details of the data protection advisor are published
- The FDPIC is notified

# Appointment of a data protection advisor – to do

**To do** - Determine whether it makes sense for your organization to appoint a formal data protection advisor (recommended for companies performing high-risk processing activities)



- Ensure that all requirements are fulfilled to benefit from the exemption
- Designate the DPA in writing (recommendation)
- Provide the DPA with
  - the necessary resources,
  - access to all information, documents, inventories of processing activities and personal data that the data protection advisor requires in order to fulfill his or her duties,
  - the right to inform the highest management or administrative body in important cases.

**! Note** - Regardless of whether a data protection advisor is appointed, it is recommended to determine the roles and responsibilities within your organization concerning data protection to ensure compliance with the requirements.

# Information – Privacy Notice

**Requirement** - The controller shall adequately inform data subjects about the direct or indirect collection of personal data.

**Exceptions and restrictions** - No information if

- ✗ data subject already has the information
- ✗ processing is provided for by law
- ✗ controller is bound by a legal obligation to secrecy
- ✗ indirect collection, where information is not possible or requires a disproportionate effort

**Restriction, postponement, or waiver** if, for example,

- ◆ measure is required by overriding interests of third parties
- ◆ information prevents the fulfilment of the purpose of the processing or
- ◆ controller has overriding interests and does not disclose the data to third parties (not group companies)



# Information – Privacy Notice – to do

## To do

### Determine who needs to be informed

- e.g., website users, employees, job applicants, customers, suppliers, consumers, patients, etc.

### Ensure that your privacy statements contain the required information

- Controller's identity and contact information (legal representative, DPA)
- Purpose of processing
- Recipients or categories of recipients of personal data
- Categories of personal data (if collected indirectly)
- For cross-border data transfers, the state and applicable transfer mechanisms/exceptions
- Automated individual decisions – decisions based exclusively on automated processing which have legal effects on the data subjects or affect them significantly
- Any other relevant information ensuring transparency and the exercise of the rights of the data subjects

### Respect the deadlines

- 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)

### Inform with a dedicated privacy notice

- e.g., website privacy notice, cookie notice, customer, and supplier notice, employee notice, job candidates notice
- via website, app, contracts, T&C, disclaimer in e-mails, invoices, order forms, etc.

# Record of processing activities – YES or NO?

**Requirement** - Controllers (and processors) must keep a record of their processing activities (RoPA).

## Minimum content:

- 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 (as of 1 January) and
- data processing is associated with a low risk for the data subjects (no extensive processing of sensitive personal data, no high-risk profiling)

# Why should you keep a record of processing activities?

Basis for Privacy by Design (Art. 7 FADP)

Basis for DPIA (Art. 22 FADP)

Basis for privacy notice and response to data subject access requests (Art. 19-21, 25 FADP)

Basis for handling data breaches (Art. 24 FADP)

Basis for data flow management/IGDTA (Art. 16 FADP)

Basis for data management and compliance

# Record of processing activities – to do

## To do

- Determine if your organization falls under the exception – if you decide not to keep a RoPA, document the reasoning
- Get an overview of your filing systems and processing activities, corporate, and function by function
- Document the processing activities and the filing systems using a template/tool (excel, word, specific tool) – with support of specific functions (HR, IT, Marketing, etc.)
- Assess the entries for completeness and compliance with data protection requirements (compliance check)
- Assess if a particular processing activity requires a data protection impact assessment (DPIA) – if yes, perform such DPIA and keep the documentation for at least two years.
- Allocate responsibilities at functional and corporate level to establish and maintain the RoPA
- Establish a process to regularly review the RoPA, and perform amendments

# 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).
- For automated processing of sensitive data on a large scale or high-risk profiling, the data controller and the processor must keep a **log** and create **processing policies**.

# Security principles and goals

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

Determine the protection needs of the personal data

## Criteria for assessing the need for protection

- The types of data processed (data classification), and
- The purpose, nature, scope and circumstances of the processing

Determine the risk to the personality or rights of the data subjects

## 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

Determine the TOMs appropriate to the risk

## 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)

# Record/Log

## Requirements

Record, at least, the storage, alteration, reading, disclosure, deletion and destruction of the data if

- sensitive personal data is processed automatically on a broad scale or
- high-risk profiling is carried out and
- the preventative measures cannot guarantee data protection

Provide minimum content

- The identity of the person who carried out the processing
- The nature, date, and time of the processing and, if applicable, the identity of the recipient of the data

Keep the records for a minimum time

- At least one year separately from the system in which the personal data is being processed
- Limited access to the logs must be ensured (need-to-know)

# Processing Policy

## Requirements

Create a processing policy for automated processing if

- sensitive personal data is processed on a broad scale, or
- high-risk profiling is carried out

Content

- Information on the internal organization, the data processing and control procedure and the measures taken to ensure data security

Regular updates

- Establish a process to regularly update the processing policy
- Make the processing policy available to the DPA, if appointed



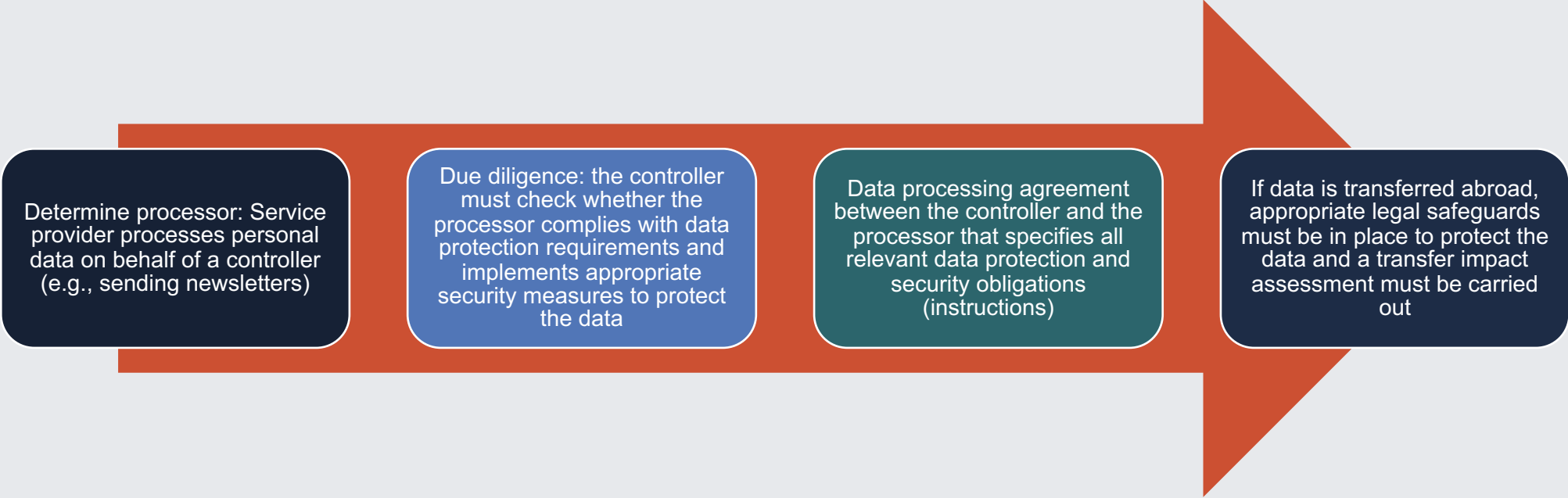
# Data security, record/log and processing policy

- Review your data security standards
  - Determine your data protection needs
  - Determine the risks for data subjects
  - Implement adequate TOMs appropriate to the identified risks
- Assess if a record and/or processing policy is required (best based on the RoPA), if so:
  - Establish a mechanism to ensure appropriate records and keeping them for at least one year, separate from the systems in which personal data is being processed (e.g., via separate back-up or automated storage in the cloud or other server)
  - Gather the required information for the processing policy and document using a form (references to existing documents!)
  - Establish a process regarding the records, and processing policies, with allocation of responsibilities

# Outsourcing

## Requirements

- 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 itself, and
  - no legal or contractual confidentiality obligation prohibits the assignment.
- The controller must ensure that the processor is able to guarantee security.
- The processor may only transfer the processing to a third party with the prior approval of the controller.



Determine processor: Service provider processes personal data on behalf of a controller (e.g., sending newsletters)

Due diligence: the controller must check whether the processor complies with data protection requirements and implements appropriate security measures to protect the data

Data processing agreement between the controller and the processor that specifies all relevant data protection and security obligations (instructions)

If data is transferred abroad, appropriate legal safeguards must be in place to protect the data and a transfer impact assessment must be carried out

# Cross-border disclosure of personal data

The cross-border disclosure of personal data remains restricted

Adequate country

Guarantees  
(e.g., BCRs, SCCs)  
and  
Transfer Impact  
Assessment

Exceptions

# Outsourcing and cross-border data transfer – to do

- Get an overview of all your service providers and data flows (within and outside your organization) and determine which service providers are your data processors (location, services, types of data, subcontractors?)
- Review existing contracts and evaluate whether they are designed to be privacy compliant
  - ✗ Insert the appropriate data protection clauses (e.g., adapted GDPR templates)
- Make sure the service provider can guarantee data security (best using a service provider assessment questionnaire)
- If the service provider is abroad, make sure that this transfer is legitimate (EU SCCs with Swiss addendum, transfer impact assessment)
- For internal data transfers, perform transfer impact assessments, if required, and establish an intragroup data transfer and processing agreement covering all possible data transfers and TOMs (or BCRs)

# Data protection standards and processes





























To ensure compliance within your organization,

- **Implement a data protection policy** outlining the general privacy principles, roles and responsibilities, and **processes** for handling, and documenting
  - data subjects' access requests or other requests regarding data protection rights (such as the right to erasure, correction, data portability)
  - data security breaches, including notifications to the FDPIC (via portal) and data subjects
  - privacy by design
  - outsourcing and cross-border data transfer
  - data storage and deletion
  - regular review of compliance with data protection requirements
- **Implement directives/SOPs regarding data protection compliance, security, and governance**, train all employees, and consider obtaining a confidentiality/data secrecy confirmation from employees that regular process personal data

# Checklist - Summary of recommendations

 personal liability (Art. 60-62 FADP)

 priority

	Assess if the new FADP applies to your organization.	
	Conduct a data management and compliance analysis to identify potential gaps, risks, and required actions.	
	Assess if a representative must be appointed in Switzerland – if so, appoint!	
	Determine if it makes sense to appoint a data protection advisor.	
	Determine who needs to be informed, review and amend your privacy notices (or create new ones) and inform while respecting the deadlines.	
	Establish a RoPA (consider exemptions!) and a process to conduct compliance assessments, DPIAs, and for keeping the RoPA up to date.	
	Determine if a legal basis is required for specific data processing (legitimate interest, consent, contract).	
	Perform compliance checks and establish if DPIAs are required (and if so, perform them).	
	Review your data security safeguards; conduct assessments to determine the level of protection and implement risk-based TOMs; determine if records/logs and processing policies are required (and if so, implement).	
	Review your relationship with vendors and associated data flows and take appropriate actions (amend contracts, perform vendor assessments, establish data transfer mechanisms, and perform transfer impact assessments). Establish a process and allocate responsibilities for ensuring compliance with the legal requirements.	
	Determine the internal data flows, and implement appropriate transfer mechanisms (e.g., IGDTPA, BCR).	
	Establish a process, and responsibilities, for handling data subjects' access requests and other requests regarding data protection rights.	
	Establish a privacy policy/directive with standards, governance, and instructions, and processes for data security, and handling, notifying, and documenting data security breaches, privacy by design, data storage and deletion, regular review of compliance with data protection requirements, IT acceptable use policies regulating the use of company devices and electronic communications, digital tools, marketing, etc..	
	Implement policies/directives/SOPs, train employees, and consider obtaining a confidentiality/data secrecy confirmation.	

# Questions?

Daniela Fábíán Masoch  
FABIAN PRIVACY LEGAL GmbH  
[www.privacylegal.ch](http://www.privacylegal.ch)

daniela.fabian@privacylegal.ch

