usercentrics

Switzerland's Act on Federal Data Protection (FADP): What You Need To Know

Overview

- Goes into effect September 1st, 2023, no grace period for compliance.
- Consent not required for data collection/processing under all circumstances.
- Applies to natural persons (no longer to legal persons) and commercial and noncommercial entities that process the data of Swiss citizens.
- Entities are responsible for compliant data processing even if they use third parties (like vendors) to do it.
- All processors must take reasonable organizational and technical measures to ensure data privacy and security.
- Applies to data in both physical and electronic files.
- Extraterritorial law, entities processing personal data do not have to be based in Switzerland.
- Prohibits transfers of personal data from Switzerland to countries with which they do not have an adequacy agreement unless explicit user consent has been obtained from data subjects.

Consent Requirements

Unlike the GDPR, the FADP allows entities to process personal data without a specific legal basis, unless the processing meets certain criteria. Consent is required for:

- processing of sensitive personal data
- processing used in high-risk profiling by a private person
- processing used for profiling by a federal body (government)
- data transfers to third countries where there is not adequate data protection

The FADP does allow for other legal bases for processing besides consent (like the law or overriding public interest), but fewer than the GDPR does. When consent is required, it must be obtained before or at the point of data collection. Like the GDPR, user consent under the FADP must be granular, informed, and voluntary.

A consent management platform enables compliant user notification, e.g. populating a privacy policy page, as well as collecting and storing compliant consent. Multiple configurations can be used with geolocation to ensure compliance with multiple regulations with different requirements, like the GDPR and FADP, depending on user location.

Notification Requirements

Data subjects must be informed at all times prior to data collection, even if consent is not required for the intended data processing.

Companies need to clearly communicate the following information to users, e.g. in a privacy policy page on the website. These are the same notification criteria required for consent to be valid:

- identity of the data controller, whether the company or a third party
- contact details for the data controller
- identity of the data recipient and any other parties involved with the data file
- recipient country if the data will be transferred cross-border
- purpose(s) of data collection and use
- what categories of data are collected, if relevant
- means of data collection, if relevant
- the legal basis for processing, if needed
- users' rights regarding their personal data under the FADP, including the right to refuse or withdraw consent

Data subjects' rights

Data subjects have the following rights under the FADP:

- request to know if data about them is or has been processed (cannot waive the right to information in advance)
- request access to their collected data
- receive their data in physical format (printed or photocopied) free of charge
- request that their personal data be corrected if inaccurate or incomplete (can be restricted, refused, or deferred, including in matters of security, to protect criminal investigations, or to protect the interests of overriding third parties)

Checklist for FADP compliance

- ✓ Create privacy statements, like a privacy policy page on the website, or update existing ones and ensure they are customized for your business, users, processing purposes, and the data you process.
  - Data subjects must always be notified re. processing even when consent is not required.
  - A consent management platform enables customizing and populating your privacy policy, as well as keeping it updated.
- ✓ Ensure notification information includes with which countries personal data is shared.
  - If there is no adequacy agreement with those countries, make that clear and get explicit consent for data sharing.
- ✓ Obtain and securely store user consent when required, e.g. for sensitive personal data processing.
- ✓ Create or update internal data processing guidelines and ensure they are well communicated.
- ✓ Set up and maintain an internal registry of data processing activities.
- ✓ Implement a process to enable efficient receipt, acknowledgement, and response to data subjects' exercising their rights, e.g. requests for copies of personal data or for correction or deletion.
  - Ensure data is portable in an accessible format, e.g. printout or common electronic format.
- ✓ Implement a data protection impact assessment, especially if the organization extensively processes sensitive data.
- ✓ Implement a process for data breaches, including prompt notification of the FDPIC and data subjects if needed. Include third parties that access or process data as well.
- ✓ Review and update contracts with third parties (like vendors) to ensure reasonable requirements for security and data privacy are met. (Though legal responsibility lies with the first party.)
- ✓ Maintain data only for as long as necessary under the stated notification, and for the stated purpose of processing. Delete or anonymize it as soon as it is no longer required for that purpose.
- ✓ Appoint a data protection officer who liaises with users and the FDPIC, and administers policies and processes.
- ✓ Consult with qualified legal counsel regarding your organization's responsibilities under the FADP and how to fulfill them. Update them regularly. Usercentrics does not provide legal advice but only information for educational purposes.