WENGERPLATTNER

Corporate and Commercial / IP & IT - March 2021

The revised Swiss Data Protection Act (FADP): Changes and their impact on companies

Authors: Dr. Tobias Meili, Melanie Müller, Dr. Martina Braun

In fall 2020, the Swiss Parliament adopted the total revision of the Federal Act on Data Protection (FADP). The revised FADP is expected to enter into force mid-2022. The purpose of the total revision is to bring the FADP into line with the rapid changes in technology, the changed social circumstances, and the General Data Protection Regulation of the European Union (GDPR) that entered into force in 2018.

An overview of the main aspects:

- **Continued application of the previous principles of data processing.**
- **Timely erasure or anonymisation of personal data remains important.**
- **Introduction of the obligation to maintain an inventory of data processing activities.**
- **Expansion of the duty to provide information when collecting personal data.**
- **Expanded requirements with respect to contract data processing.**
- **Data breaches may now be punished with fines of up to CHF 250,000.**

The revised Swiss Data Protection Act (FADP): Changes and their impact on companies

Dr. Tobias Meili
Partner in the Corporate and Commercial practice area and on the IP and IT team, Attorney at Law
tobias.meili@wenger-plattner.ch

Melanie Müller
Associate on the Life Sciences and Health Law as well as the IP and IT team, Attorney at Law
melanie.mueller@wenger-plattner.ch

Dr. Martina Braun
Senior associate on the IP and IT team, Attorney at Law
martina.braun@wenger-plattner.ch

Personal data is a valuable asset. Due to the constantly evolving technologies and the opportunities resulting thereof, as well as with regard to the introduction of the GDPR, it became necessary to bring Swiss data protection law in line with current conditions. The revised FADP enhances data protection to a significant degree, which is likely to lead to a need for action on the part of Swiss companies regarding internal processes and security measures.

Introduction

It is imperative that the new regulations are addressed in time since, with few exceptions, the revised FADP does not contain transitional provisions. Most of the changes will apply immediately once the revision enters into force. Exceptions will apply solely with respect to technical data security measures (privacy by design and privacy by default), as well as in the area of data protection impact assessments.

Scope of application

The FADP applies as before to all companies that have a registered office in Switzerland or whose data processing has an impact in Switzerland, regardless of the size, legal form, or type of business activity.

Applicability of previous principles

The previous principles continue to apply. In particular, in the private domain (as contrasted with processing by federal bodies), the principle continues to apply that for the processing of personal data, in general neither a consent nor any other legal justification is required, which is different from the GDPR. Further, data must be destroyed (or erased in compliance with data protection requirements) or anonymised as soon as they are no longer necessary for the purpose of the processing. As before, these principles result from the requirement of proportionality of data processing.

Overview of important changes

General

To date, the FADP applies to natural persons and to legal entities. Henceforth, its scope will be limited to the data of natural persons, which is the same as under the GDPR.

Privacy policy

Many companies have already devised a privacy policy in accordance with the GDPR. As a result of the expanded duties to provide information, such a privacy policy is also essential under the revised FADP. Privacy policies formulated in accordance with the GDPR are usually very extensive but may be used with corresponding adjustments. The revised FADP will require that when personal data is collected, data subjects must be advised of the following: the identity and contact details of the controller, the purpose of processing, if applicable the categories of recipients and data and, in the event that personal data will be disclosed abroad, the states in question and, if applicable, protection measures (see below). The privacy policy can, for example, be posted on the company website.

Do I need a data protection officer (DPO) in my company?

A DPO or data protection officer (in future «data protection advisor») may be necessary in certain companies if, for example, data processing is a core activity of the company. In Switzerland, a company can appoint an employee or a third party as DPO. If a DPO is appointed, this must be reported to the Federal Data Protection and Information Commissioner (FDPIC) and be specified in the privacy policy. Usually, companies assign an employee to deal with data protection issues generally, but such employee is not automatically considered as a DPO.

Under the revised law, there is little incentive, however, to appoint a DPO: a data processing project which, once a data protection impact assessment has been conducted, continues to present a «high risk», need not be presented to the FDPIC if the DPO is responsible for the processing project. Such cases are rare in practice though. The previous advantage that a company does not have to report its data collections otherwise subject to registration to the FDPIC by appointing a DPO is eliminated under the revised FADP.

For companies subject to the GDPR, but that do not have a subsidiary in the EU, there is usually an obligation to appoint a data protection representative in an EU member state. This shall provide the supervisory authorities with an actual possibility of access to the data processing or the company within the EU. Under the revised FADP, there is an obligation for foreign companies to appoint a representative in Switzerland under certain circumstances.

Rights of data subjects

Under the revised FADP, data subjects continuously have the right to request information about their data and to request rectifications of it, as well as to object to any processing. The exercise of data subject rights is in principle free of charge. In the event of a request for information, the company must respond within 30 days, although the provision of a declaration of completeness is not required. In addition, the revised FADP provides for a right to obtain stored data or to have it transferred (right to data portability). This means that the data subjects may, under certain circumstances, request the disclosure or transfer of their personal data in a standard electronic format.

Inventory of processing activities

As under the GDPR, the revised FADP will require that an inventory be maintained that captures the various processing activities. If an inventory has already been established in accordance with the requirements of the GDPR, this will meet the conditions pursuant to the revised FADP as well. Companies are left to decide how the inventory is formally structured, an excel table will suffice, for example. The minimum content of the inventory, however, is specified by the FADP. For each data processing activity, the inventory must contain at least the following information: the identity of the controller and, if applicable, the processor, the purpose of processing, the categories of data subjects and personal data processed, the categories of recipients, the period for which the personal data will be stored or data protection measures and, if applicable, the recipient states and information with respect to protection measures.

Transfer abroad

According to the revised FADP, personal data may be disclosed abroad if the legislation of the relevant state guarantees an adequate level of protection. A transfer of data to an «unsafe country» is only permitted if equivalent data protection is otherwise ensured. This corresponds, in principle, to the previous provision. In future, the Federal Council, and no longer the FDPIC, will specify which countries are deemed to be safe. The revised FADP largely corresponds to the GDPR with respect to the possible protection measures for disclosure to «unsafe countries». Recognised special safeguards are, for example, standard contractual clauses approved by the FDPIC or group-wide binding corporate rules (BCR).

Contract processing

Any person who, as controller, delegates the processing of personal data to a third party (e.g. service provider) must conclude a contract with this third party. Such contract must regulate the instructions and monitoring rights of the controller in relation to the respective third party and contain provisions regarding the guarantee of data security. What is new according to the revised FADP is that any involvement of a sub-processor is only permitted with the consent of the controller.

Data breach notification

Under the revised FADP, controllers are required to notify the FDPIC of any data breach as quickly as possible if there is a high risk for the data subjects. In addition, they must notify the data subjects, if this is necessary for their protection. It is recommended that a specific person or entity in the company be designated to which employees are required to report incidents.

Safety measures

The principles of privacy by design and privacy by default already applicable under the GDPR are now expressly anchored in the revised FADP, i.e. controllers must, as before, make every effort to implement appropriate technical and organisational data protection measures.

« The measures required to bring your company in line with the revised FADP should be dealt with as soon as possible because upon entering into force of the FADP, a transition period is only provided for with respect to a few of the new obligations. »

Liability

Investigative proceedings due to violations of data protection provisions are directed against the person, who is responsible for the data processing in question. In contrast with the GDPR, the fines are however not directed against the relevant company. The penalty provisions were significantly expanded according to the revised FADP and the fines for breaches of data privacy have now been increased to up to CHF 250,000.00. According to some opinions, such fines, because of their personal nature, cannot be insured nor may the company pay them on behalf of the respective natural person.

Measures to take

To implement the new measures, it will be necessary in a first step to identify what personal data is collected and processed, for what purposes, how, where, and by whom. The data protection measures and procedures in place must be documented. As a next step, a review is needed to determine if and what gaps exist according to the revised FADP. Then, using a risk-based approach, it will be required to take the necessary measures such as:

- implementing the obligations to provide information by creating or adapting privacy policies;
- establishing a data processing inventory;
- entering into or amending contracts with processors;
- establishing internal processes and responsibilities to safeguard the rights of data subjects (right of information, access, rectification, erasure, and objection) and preparing internal directives and templates (e.g. for responding to data privacy inquiries);
- implementing the procedures and responsibilities in respect of personal data breaches.

Finally, it is necessary to ensure that any measures and processes established are implemented and maintained on an ongoing basis. For this, it is indispensable to (i) appoint responsible officers within the company, (ii) equip them with adequate resources and, (iii) train and support all employees, in a level-appropriate and practice-oriented manner, in accordance with their functions and the associated «proximity» to the processing of personal data.

Practical recommendations

Companies must be prepared to devote even greater attention in the future to data protection. Use this legislative revision as an opportunity to conduct a risk-based review of the data processing activities within your company with regard to their conformity with the revised FADP. Start with the implementation work at an early stage because once the law has entered into force there is only a transition period for a few of the new obligations. Also, from the beginning, make sure to involve the responsible decision-makers in the relevant areas (in particular IT, marketing and HR) in which personal data is typically processed, and also involve representatives from legal & compliance.

Basel: Aeschenvorstadt 55 | CH-4010 Basel | T +41 61 279 70 00 | basel@wenger-plattner.ch
Zürich: Seestrasse 39 | CH-8700 Küsnacht-Zürich | T +41 43 222 38 00 | zuerich@wenger-plattner.ch
Bern: Jungfraustrasse 1 | CH-3000 Bern 6 | T +41 31 357 00 00 | bern@wenger-plattner.ch

www.wenger-plattner.ch