

Banks & Financial Services

Providers

Competition Law

Construction & Real Estate Law

Corporate & Commercial Law

Data Law

Energy Law

Financial Market Infrastructure Law

Financing

FinTech

Funds & Asset Management

Immigration Law

Information Technology Law

Inheritance Law & Estate

Planning

Insurance

Intellectual Property Law

Labor & Employment Law

Litigation & Arbitration

Media Law

Mergers & Acquisitions

Notarial Services

Pharmaceutical & Health Law

Restructuring & Insolvency

Tax Law

Venture Capital & Private Equity

White-Collar Crime

Need for action due to the revised Swiss Federal Act on Data Protection

The revised Swiss Federal Act on Data Protection (FADP) was passed by parliament in the fall of 2020 after years of wrangling. Even though the corresponding ordinance is still being drafted, it is now fairly clear what is in store for businesses: New information and documentation obligations, a duty to report data breaches, and the risk of a fine if certain obligations are not met. The revised Data Protection Act is expected to come into force in mid-2022 and companies can and should use the time remaining until then to prepare for the new obligations, conduct the necessary internal investigations and implement the required measures.

Tighter documentation, auditing and reporting requirements

A significant tightening in the revised FADP will occur analogously to the GDPR in the area of documentation requirements. In principle, companies are required to keep a record of their data processing activities. Data protection impact assessments must now be carried out before processing sensitive personal data, and the FADP now includes a reporting obligation to the Federal Data Protection and Information Commissioner (FDPIC) for data protection incidents such as data loss or other types of data protection violations.

Companies that employ fewer than 250 employees and whose data processing involves a low risk of violations of the personal rights of data subjects are exempt from the obligation to maintain a processing record. This means that even companies with fewer than 250 employees may be affected by the obligation to maintain a processing record, depending on the category of the data and the nature of the data processing. Since, however, awareness of the data processing operations carried out in the

company is an essential part of the general documentation, auditing and reporting obligations, it is recommended to keep a processing record anyway.

Appointment of a data protection officer

In contrast to the GDPR, the revised FDAP does not stipulate an obligation to appoint a data protection officer. Such an appointment is voluntary. Upon appointment, the organisational and professional requirements for data protection officers mentioned in the FDAP must be met, i.e., the person in question must have the necessary expertise and be able to act independently within the organisation. The appointment of a data protection officer will often not be feasible for smaller and medium-sized companies. However, the creation of a position in charge of compliance with data protection requirements (such as the compliance officer) is likely to make sense for most companies in view of the increasingly complex requirements with regard to information and documentation obligations. The responsibility does not necessarily have to be assigned to one person, but can also be assigned to a team.

Wenger & Vieli Ltd.

Dufourstrasse 56

P.O. Box

CH-8034 Zurich

Office Zug

Metallstrasse 9

P.O. Box

CH-6302 Zug

T +41 58 958 58 58

spotlight@wengervieli.ch

www.wengervieli.ch

**CLAUDIA KELLER**

LL.M. | Counsel | Attorney at law
c.keller@wengerviel.ch
T +41 58 958 53 47

**MICHAEL TSCHUDIN**

Dr. iur. | Partner
m.tschudin@wengerviel.ch
T +41 58 958 55 47

**DOMINIQUE ROOS**

Attorney at law
d.roos@wengerviel.ch
+41 58 958 55 47

**MARCEL BOLLER**

Dr. iur. | Attorney at law
m.boller@wengerviel.ch
T +41 58 958 55 63

**SPOTLIGHT AS PDF:**

<https://www.wengerviel.ch/en-us/publications?typ=spotlight>

Disclaimer: The information contained in this document is intended for general information purposes only and does not constitute legal or tax advice. This content is not meant to replace individual advice from competent professionals in a specific case. © Wenger & Vieli Ltd., 2021

Tightening requirements with regard to the involvement of processors

Virtually all companies delegate part of the processing of personal data to a processor, first and foremost to IT service providers, which requires a data transfer. This delegation, or outsourcing in general, is subject to more stringent requirements under the revised FDAP. The most important innovation is the approval requirement for the use of sub-processors. It is therefore necessary to review and, if necessary, adapt existing contracts with contractors.

Privacy notice becomes a must

Due to the extended duty to provide information in the revised FADP, companies are obliged to proactively provide minimum information about the personal data they collect and process. As a rule, this will be achieved through the already familiar instrument of the privacy notice. Most companies already publish such a privacy notice on their website. In terms of content, this should be aligned with the minimum requirements under the revised FADP. The FADP does not prescribe specific formalities for the privacy notice. The information must be provided at the time the data is collected, i.e., instead of a comprehensive privacy notice, it is also possible to inform data subjects separately for each specific data processing activity.

Visual aids can also be used to make data privacy statements easier to understand. There are already companies that summarise their privacy notices in a video. An initiative originating from the digitalswitzerland association developed privacy icons to help companies make their respective data processing easily recognisable and comprehensible by using privacy icons in their privacy notices (www.privacy-icons.ch).*

Order and fine regime

The revised FADP gives the Federal Data Protection and Information Commissioner the possibility to issue orders regarding specific data processing operations against companies. In addition, the cantonal criminal authorities can now impose a fine for certain intentional violations of the revised FDAP up to an amount of CHF 250,000.

What are the essential to dos?

- **Create a processing record:** As a source central for the content of the privacy notice, for the implementation of measures based on data protection impact assessments, review of contracts with processors, and for the obligation to notify data protection breaches.
- **Adaptation of the privacy notice:** For the use of the website and the business relationship in general, possibly considering the use of privacy icons.
- **Development and implementation of a concept regarding data subject access requests (SAR):** Assignment of responsibilities and instructions on how to process requests for information (audit and documentation obligations) due to short legal deadlines to respond to such SAR.
- **Adjustment of contracts with processors:** In this context, special attention must be paid to any data transfers abroad.
- **Development and implementation of a concept for data protection impact assessments:** For new projects, data protection know-how should be involved at a relatively early stage.
- **Development and implementation of a data protection breach concept:** The effort involved in clarifying the matter and taking measures, including notification to the FDPIC, should not be underestimated. The notification to the FDPIC must be made "as soon as possible".

Further measures are particularly necessary if sensitive personal data is processed or automatic decision-making based on personal data takes place. In principle, there is no one-size-fits-all solution, but the risk-based approach inherent in data protection law means that the necessary measures must be based on the risk that the specific data processing poses to the personal rights of the data subjects.

Also, non-Swiss companies may be subject to the obligation to appoint a Swiss representative similarly to the requirement of an EU representative under GDPR.

* Wenger & Vieli AG is a founding member of digitalswitzerland and the Privacy Icons association.