suterhowald
Rechtsanwälte
Attorneys at Law

NEWSLETTER

MAY 2023

Author: Dr. Urs Egli

The revised Federal Act on Data Protection

The revised Federal Act on Data Protection (FADP) will come into force on September 1, 2023. The revision aims to align the FADP with the European General Data Protection Regulation (GDPR). Companies that have not yet implemented a program to ensure GDPR compliance must adapt their governance protocols.

I. Revision

On May 25, 2018, the European General Data Protection Regulation (GDPR) entered into force. This and technological developments set a comprehensive revision of the Federal Act on Data Protection (FADP) in motion. The FADP applies to private companies as well as to federal authorities. Cantonal authorities and institutions are subject to cantonal data protection laws.

The FADP outlines rules on personal data processing and defines the rights of the persons concerned. Certain provisions of the FADP provide for sanctions under criminal law.

The FADP will enter into force on September 1, 2023. It has been comprehensively revised and restructured. On the same date, the revised Ordinance to the Federal Act on Data Protection (DPO) will also come into force, which also includes provisions on information security.

II. Terminology

The previous "controller of the data file" is now referred to as the "controller" and the person whose data is processed as the "data subject". Companies that process personal data on behalf of the controller are "processors". Under the GDPR, the contract between the controller and the processor is referred to as a "*data processing agreement*"; consequently, in Switzerland, the same term is used.

III. Contents

1. Preliminary remarks

Most of the provisions of the revised Data Protection Act were already applicable under the previous law, but some of them have been expanded (section 2). Others are new (section 3).

2. Continuation and expansion of existing regulations

2.1 Personal data

Only personal data, i.e., information relating to an identified or identifiable natural person, is protected by the revised FADP (in contrast to the previous FADP, which also covered the protection of data relating to legal persons). Pseudonymized or encrypted data is personal data only if the data can be associated by the controllers or processors with an identified or identifiable individual. Therefore, a transfer of

encrypted data to a processor abroad is not considered a cross-border data transfer so long that the processor does not have access to the encryption key.

If data anonymization can only be reversed by way of disproportionate means, anonymized data is also not considered personal data, as the data can no longer be attributed to a specific individual. In such cases, the anonymization of data is equivalent to the deletion of data in terms of data protection law.

2.2 Processing principles and justifications

According to Art. 6 FADP, the processing principles are lawfulness, proportionality, purpose limitation and transparency as well as data accuracy.

According to Art. 31 FADP, the grounds for justification are the consent of the data subject and an overriding private or public interest.

Data processing in the private sphere is generally permissible and requires neither consent nor any other justification. In contrast to the GDPR, such a reason is only required if either the processing principles or the data security provisions are not complied with or if the data subject objects to the processing.

2.3 Consent

The data subject's consent is required in some situations. The two most important constellations are the cross-border disclosure of data to a country without an adequate level of data protection, without appropriate protection being guaranteed by other means (Art. 17 para. 1 let. a FADP), and data processing that violates personal rights (Art. 31 para. 1 FADP). The consent must be explicit. It is not required to be in writing.

2.4 Right of access to information

The data subject has the right to request information from the controller as to whether and what personal data about them is being processed. Art. 25 FADP describes the content of the information in more detail than under the previous law. The information can be refused if the request is not made in good faith or obviously unfounded, i.e., pursues a purpose contrary to data protection. With this clarification, it is questionable whether data protection law can continue to be misused to obtain evidence, as was previously possible based on federal case law in this regard.

2.5 Right of objection

The data subject has the right to object to the processing of their data (Art. 30 para. 2 let. b FADP). By exercising the right of objection, further processing of their personal data becomes inadmissible, unless the controller has sufficient grounds for justification.

2.6 Right of correction and deletion

The data subject has a right of correction with regard to inaccurate data as well as a right of deletion (Art. 32 FADP).

2.7 Disclosure requirements and privacy policy

The disclosure requirements for the collection of personal data are significantly expanded in the new FADP (Art. 19 FADP). They now apply generally and are no longer limited to the collection of sensitive personal data. Information must be disclosed on the identity and contact information of the controller, the purpose of processing, the recipients of personal data (if applicable) and, in the case of cross-border data disclosure, the name of the State or international body. Recipients refers to third parties who have access to data, whereby it is sufficient to designate them as a category (e.g., disclosure to processors or corporate affiliates).

The form of information is not prescribed by law. It is usually disclosed in form of a privacy policy on the organization's website, which can be referenced in the GTC or other documents.

2.8 Data security

As before, the controller and any processors must ensure risk-appropriate data security by means of suitable technical or organizational measures (Art. 8 FADP). The minimum data security requirements are outlined in the DPO. The controller is required to take such technical and organizational measures as necessary and appropriate with regards to the data processing purpose, risk, prevailing technical standards and the implementation costs. The DPO lists specific protection objectives (e.g., access controls, entrance control, data carrier controls, storage controls, usage controls, recovery). It however is the concerned companies' responsibility to determine what constitutes adequate data security.

2.9 Data processing by processors

The processing of data may only be assigned by agreement or by legislation (Art. 9 FADP). In addition, the processor may now only assign the processing to

a third party with the prior authorization of the controller (Art. 9 (3) FADP). Both provisions have been adopted from the GDPR.

2.10 Cross-border data disclosure

As before, personal data may be disclosed abroad only if the legislation of the relevant State or international body guarantees an adequate level of protection (Art. 16 FADP). Data disclosure to other countries is only permitted with appropriate safeguards being in place. The simplest way is to use the standard contractual clauses of the European Commission, which have been approved by the Federal Data Protection and Information Commissioner (FDPIC) and adapted for use under Swiss data protection law. The obligation to notify the FDPIC of the data disclosure, as was still provided for under previous FADP provisions, will no longer apply. The FDPIC does however stipulate that if the standard contractual clauses provide sufficient security or if additional provisions are necessary in individual cases must be examined on a case-by-case basis (i.e., *transfer impact assessment*).

If no such approved standard contractual clauses are used, the contract governing the disclosure must be submitted to the FDPIC (approval is not required).

It further is possible to issue internal company data protection regulations (i.e., *Binding Corporate Rules*), which however must be approved by the FDPIC in advance.

Finally, data may be disclosed abroad if it is directly related to the conclusion or execution of a contract (e.g., disclosure of the payee in the case of bank transfers) or if the consent of the data subject has been obtained (Art. 17 FADP).

3. New provisions

3.1 Inventory of processing activities

Controllers must now keep an inventory of their processing activities (Art. 12 FADP; under the GDPR called "record of processing activities"). Companies with fewer than 250 employees are exempt from this obligation, provided their processing does entail only a low risk of infringing the personality of the data subjects.

Records of processing activities that have already been created under the GDPR can be adopted. The FADP does not specify the extent to which the records must be broken down into individual processing activities. It is recommended to combine processing activities related by business function (e.g., personnel administration, recruitment, customer data management, customer service, online store, newsletter, product development, supplier management, finance and accounting, evaluation of website usage, video surveillance, facility management, finance and accounting and e-mail).

The contents of the inventory of processing activities is stipulated in Art. 12 Para. 2 and 3 FADP. A special format for the record is not prescribed. It can be maintained as an Excel or Word file or in the form of an IT solution.

Processors must also maintain their own record. As one of the processing activities, the services performed on behalf of the controllers must be listed there in a general manner (e.g., provision of IT operating services for customers).

3.2 Data protection impact assessments

Controllers planning data processing operations that may potentially involve a high risk for the data subject's personality or fundamental rights, must conduct beforehand a data protection impact assessment. Examples of high-risk data processing include the introduction of a fleet management system with real-time monitoring of vehicle locations, the creation of a database with potential job candidates by an HR department, or the maintenance of a comprehensive customer database by an online retailer.

The data protection impact assessment is a self-evaluation under data protection law. It requires analysis of potential negative consequences, corresponding probability of occurrence, possible preventive measures and FADP compliance. If the data protection impact assessment shows that the processing presents a high risk for the personality or fundamental rights of the data subject despite the measures envisaged by the controller, the controller must consult the FDPIC (or the data protection advisor) prior to the processing.

3.3 Notification of data security breaches

The controller must notify the FDPIC as soon as possible of a data security breach that is probable to result in a high risk to the personality rights or the fundamental rights of the data subject. Examples of breaches of data security include hacker attacks, e-mails containing sensitive data sent to the wrong recipient, technical errors, system errors or access by

foreign authorities to data in the cloud. Whether a high risk exists must be determined by the controller on a case-by-case basis. Examples of high risk are password theft in a hacker attack on an online store, customer data theft by a bank employee, or the loss of a user device with access to confidential data.

The reporting obligation lies with the controller. The FDPIC must be informed as soon as possible. However, unlike the GDPR, there is no specific deadline (72 hours under GDPR).

The processor is subject to a separate and more extensive reporting obligation, as he must report every data security breach, regardless of risk level. However, the processor must report to the controller and not to the FDPIC. This is a legal obligation that can neither be contractually waived nor limited.

3.4 Data protection advisor

A data protection advisor pursuant to Art. 10 FADP is intended as a contact point for data subjects and the authorities. He advises the controller on data protection issues and conducts training. The appointment of a data protection advisor under the FADP, different from the GDPR, is voluntary for private controllers. The only tangible advantage of a data protection advisor is that FDPIC consultation is not required when a data protection impact assessment indicates high risk.

3.5 Data protection representative

Foreign controllers without a registered office or domicile in Switzerland must under certain circumstances designate a representative in Switzerland for data protection matters (Art. 14 FADP).

3.6 Profiling

Profiling is defined as automated data processing that assesses certain personal aspects relating to a natural person. If the combining of such data allows for the assessment of essential aspects of the personality of a natural person, then this constitutes high-risk profiling, for which explicit consent is required (Art. 6 para. 7 let. B FADP).

3.7 Automated individual decisions

Automated individual decisions are decisions that are made exclusively by a machine and that significantly impact the person concerned. Examples are the automatic pre-selection of job applicants or the granting of loans. The data subject must be informed about such decisions and given the opportunity to have the decision taken reviewed by a natural person (Art. 21 FADP).

3.8 Right of data portability

Pursuant to Art. 28 FADP, a data subject may request the surrender of data processed by the controller in an automated manner, if the data is processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject. The original aim of this provision was to enable social media users to switch to another provider. The extent to which this provision also applies to other circumstances (e.g., claim for data surrender against cloud providers) remains to be seen.

4. Reporting and registration obligations

The registration obligation for data collections was abolished. The obligation to report cross-border disclosures of data to the FDPIC whenever the destination country does not have adequate data protection has also been abolished. However, the standard contractual clauses used must be reported to the FDPIC, if they were not already approved earlier.

The appointment of a data protection advisor (which itself is not mandatory) or, if applicable, of a representative for foreign controllers must be reported to the FDPIC. In addition, the FDPIC may have to be consulted in connection with data protection impact assessments.

5. Sanctions

The enforcement of crucial FADP obligations includes provisions for sanctions under criminal law. This applies to violations of information and disclosure obligations, unlawful cross-border data disclosure, processing without a processing policy, noncompliance with minimum data security requirements and to the violation professional confidentiality.

The penalty is a fine of up to CHF 250,000. Sanctions apply only to the natural persons responsible (e.g., managers, data protection advisors). Only intentional violations are punishable. The company can only be fined in exceptional cases where the identification of the responsible natural person would involve disproportionate effort (Art. 64 FADP).

6. Transitional provisions

Data processing that was previously permitted will in principle also be permitted after the revised FADP comes into force. It is also not required to conduct

data protection impact assessments for data processing that is already ongoing when the FADP comes into force. However, the data protection organization and the data protection policy must be adapted to the new requirements of the FADP.

The requirements of the FADP must be complied with immediately upon its coming into force. There will be no grace period.

7. Recommendations

We recommend the following measures to private companies:

(1) Review the **privacy policies**.

(2) Determine the **organizational responsibility** for data protection.

(3) Document the **data security**.

(4) Create an **inventory of processing activities.**

(5) Verify that a **data processing agreement** is in place for all **processing** carried out by third parties.

(6) Identify and secure **data disclosures to insecure third countries.**

(7) Define the following **responsibilities and processes** and document this in an appropriate form (**regulations**, BoD resolution):

- Processing of requests for information, correction and deletion and of objections to data processing;
- Data processing impact assessments;
- Data security breach reporting;
- Deletion and archiving of data.

(8) Inform the employees of their **professional confidentiality** obligations.

For companies that have already adapted their organization to the GDPR, the revised FADP brings only a few changes.

The content of this newsletter does not constitute legal advice and may not be used as such. For personal advice, please contact your contact person at Suter Howald Attorneys at Law or the following person:

Dr. Urs Egli
Counsel

urs.egli@suterhowald.ch

Suter Howald Attorneys at Law

Räffelstrasse 26 | P.O. Box | CH-8021 Zurich