The revised Federal Act on Data Protection

15.01.2021

Key takeaways

- **The referendum deadline has expired unused: the revised Swiss FADP is expected to come into force in mid-2022.**
- **The revised FADP introduces various new obligations for data controllers and processors, such as a comprehensive duty to provide information or a duty to record data processing activities.**
- **Intentional non-compliance with certain data protection provisions can be punished by a fine of up to CHF 250,000. This penalty is not imposed on the company, but on the person responsible for the data protection violation.**
- **As there are hardly any transitional periods, implementation of the new provisions requires planned and immediate action: (i) adapt your privacy policies and GTCs; (ii) adapt your DPAs; (iii) check whether data transfers to third countries without adequate data protection levels are based on sufficient guarantees; (iv) create a record of processing activities; (v) create standard templates for reporting data breaches; (vi) create standard templates for responding to requests for information.**

1. Revised FADP is a done deal

After a legislative process lasting more than four years, the deadline for calling a referendum against the revised Federal Act on Data Protection (reFADP) expired unused on 14 January 2021. The reFADP and the new data protection regime it introduces will therefore likely come into force by mid-2022 at the latest.

Pestalozzi Rechtsanwälte AG
Feldeggstrasse 4
CH-8008 Zürich
T +41 44 217 91 11
zrh@pestalozzilaw.com

Pestalozzi Avocats SA
Cours de Rive 13
CH-1204 Genève
T +41 22 999 96 00
gva@pestalozzilaw.com

pestalozzilaw.com

2. Comprehensive obligations for data controllers and processors

The good news first: the regulation concept of the reFADP remains the same. In contrast to the EU's General Data Protection Regulation (GDPR), the processing of personal data in the private sector still requires neither consent nor any other justification. A justification is only necessary if the processing principles are not complied with; the data subject has objected to the processing; or a third party is to be provided with sensitive personal data.

Nevertheless, with the reFADP, the legislator introduces various new obligations for both data controllers (controllers) and processors (processors). These new obligations and the reFADP in general may also apply to companies based abroad, in particular if they process personal data and this data processing has an impact in Switzerland.

The most important of the new obligations and the resulting need for action for controllers and processors are listed below:

Comprehensive obligations for data controllers and processors

Obligation	Need for action
Obligation to provide comprehensive information: • Subject to certain exceptions, controllers have a duty to inform a data subject whenever its personal data is collected. • Information must be provided on the identity and contact details of the controller, the purpose of the processing and the categories and locations of recipients to whom the data are disclosed.	• Companies have to align their privacy policies with the new information requirements. The website or brochures, forms and general terms and conditions must refer to these revised policies. • Existing customers do not need to be proactively informed. It is sufficient to inform them as soon as their personal data are next processed.
Obligation to keep records of processing activities: • Controllers and processors are each obliged to keep records of data processing activities under their responsibility. • The record of the controller must contain the following information: (i) identity of the controller; (ii) purposes of the processing; (iii) description of the categories of data subjects and of the categories of personal data; (iv) categories of recipients; (v) retention period; (vi) description of the measures taken to guarantee data security; and (vii) identification of third countries to which personal data is disclosed. • The record of the processor must contain the following information: (i) identity of the processor and the controller; (ii) categories of processing carried out on behalf of the controller; (iii) description of the measures taken to guarantee data security; and (iv) identification of third countries to which personal data is disclosed.	• Companies, which already keep records in accordance with the requirements of the GDPR, must supplement such records with the following information: (i) countries to which data is disclosed; and (ii) guarantees on which the controller bases the transfer of data to countries without adequate data protection level. • Companies which do not yet have a record of data processing activities must introduce one. The record must contain the information required by law, document all data processing activities and be kept up to date.

Obligation to obtain prior consent for sub-processing: • Processors may only assign the data processing to a third party (sub-processor) with the prior authorisation of the controller. • This regulation also applies to the use of sub-processors within the group. There is still no group privilege in this respect (the same applies to the additional requirements concerning cross-border data disclosure).	• Data processing agreements (DPAs) that comply with the GDPR can be used, but must be adapted as follows: (i) supplementing the references to the GDPR with references to the reFADP; (ii) adapting the rules on disclosure of data abroad so that data exports from Switzerland are also covered; and (iii) formulating the scope in such a way that in international relations all contractual data processing under the reFADP are covered and not only those subject to the GDPR. • DPAs failing to provide that sub-processors may only be engaged with the prior authorisation of the controller must be supplemented with such an authorisation mechanism.
Obligation to secure personal data: • Controllers must ensure that the technical systems used for data processing are designed to comply with the principles of Swiss data protection law (‘privacy by design’). • Further, controllers must ensure, by appropriate pre-settings, that the processing of personal data is limited to the minimum required for the intended purpose (‘privacy by default’).	• Controllers (and processors) must implement ‘state of the art’ technical or organisational measures in good time to ensure data protection, for example, by means of automated data deletion, access restrictions, issuing of appropriate regulations and instructions. • In case controllers provide several variants of how data can be processed in a service, software or device, default settings must be defined so that processing is limited to the minimum necessary for the intended purpose.

Obligation to carry out a data processing impact assessment: • Controllers are obliged to carry out a data protection impact assessment (DPIA) on any new project likely to involve a high risk to the personality or fundamental rights of the data subject. • DPIAs must be prepared before beginning any data processing activity. • Controllers may abstain from establishing a DPIA, for example, if they use a system, product or service that is certified for the intended use by a recognised independent certification organisation.	• Unless there is an appropriate certification, controllers must carry out a DPIA when a data processing activity by its nature is likely to present a high risk to the personality of the data subject. This may be the case, for example, with systematic surveillance, processing of confidential or highly personal data, profiling, or automated individual decisions. • If the high risk of data processing cannot be countered by technical or organisational measures, the relevant project must be submitted for consultation to the Federal Data Protection and Information Commissioner (FDPIC) or, if one has been appointed, to the data protection adviser (other options reserved).
Obligation to notify data security breaches: • If, in the course of data processing, the confidentiality, integrity or availability of personal data is affected in an unforeseen manner and this result in a high risk of personal data being lost, deleted, altered, disclosed, or made available to unauthorised persons (data breach), the controller may be obliged to report this data breach to the FDPIC. • This obligation to report to the FDPIC is the sole responsibility of the controller. A processor is subject to own reporting obligation vis-à-vis the controller: the processor must report any breach of data security that comes to his attention. This applies regardless of whether such breach involves a high risk. • There is no ‘de minimis’ rule. Even if only one person is affected by a data breach, a notification may be required.	• In case there is an obligation to report the data breach, the controller must notify the FDPIC as soon as possible. There is no time limit of 72 hours as under the GDPR. • The obligation of the processor to report breaches exists by law and does not require a contractual agreement. However, such an explicit agreement is recommended. • Controllers should inform the data subjects of a data breach when this information is necessary for their protection. This is the case when data subjects have to take action to protect themselves from the consequences of the data breach or to mitigate them.

Obligation to appoint a representative: • Companies without a registered office in Switzerland may be obliged to appoint a representative in Switzerland if (i) they process personal data of persons in Switzerland; (ii) they offer these persons goods or services or observe their behavior in Switzerland; (iii) processing of such data is extensive and takes place on a regular basis; and (iv) according to the DPIA, processing involves a high risk for the personality of the data subjects.	• Companies appointing a representative must notify the representative to the FDPIC and provide the contact details of the representative in privacy policies. • The representative must keep a record of the processing activities of the controller.

3. Non-compliance may result in fines of up to CHF 250,000

The reFADP not only introduces new obligations but also provides for increased penalties in case of non-compliance. In future, the intentional infringements of certain data protection provisions, for example, non-compliance with the information obligations, will be punishable by fines of up to CHF 250,000.

In contrast to the GDPR, it is not the company that is penalised, but the person responsible for the data violation. This person does not necessarily have to be a manager. It can also be someone who is not a member of a corporate body, but who is in charge of the relevant proceedings, such as the company DPO or the external legal counsel who, for example, decides on the privacy policy.

4. No transition periods – immediate action required

As the FADP provides for hardly any transitional periods, companies subject to the reFADP will be obliged to comply fully with the newly introduced obligations as soon as it enters into force. Companies affected should therefore take a forward-looking approach and begin the process of implementing the new provisions today. The following steps are recommended:

In a first step, companies should establish their starting position under data protection law: Whose data do we process, which types of personal data, and for which purposes? What is the potential justification for our data processing? Do we disclose personal data to third parties? Do we disclose personal data cross-border to countries without an adequate level of data protection? On what guarantees do we base such cross-border data disclosures.

In a second step, companies should define the gaps between the actual and target status and the resulting need for action. The concrete need for action and the time needed for its implementation depend to a large degree on the extent to which the company concerned already complies with the GDPR provisions today.

As it is unlikely that the measures necessary to meet the need for action can be implemented simultaneously, it will be necessary in a third step to set priorities for the realisation of these measures. In this context, it might be useful for a company to implement measures that protect it from possible sanctions under the reFADP in advance. Priority should be given to the following actions: (i) adaptation of privacy policies and GTCs to meet the information obligation; (ii) adaptation of DPAs; (iii) review and, if necessary, adaptation of guarantees to ensure an adequate level of data protection in case of data transfers to third countries (keyword: Schrems II); (iv) creation of records of processing activities; (v) creation of standard templates for reporting data breaches; and (vi) creation of standard templates for responding to requests for information.

With our long-standing and proven professional expertise, Pestalozzi Attorneys at Law is at your disposal during both the evaluation and implementation process.

Contributors: Michèle Burnier (Partner), Nando Lappert (Associate)

No legal or tax advice

This legal update provides a high-level overview and does not claim to be comprehensive. It does not represent legal or tax advice. If you have any questions relating to this legal update or would like to have advice concerning your particular circumstances, please get in touch with your contact at Pestalozzi Attorneys at Law Ltd. or one of the contact persons mentioned in this Legal Update.

© 2021 Pestalozzi Attorneys at Law Ltd. All rights reserved.

Michèle Burnier

Partner
Attorney at law

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland
T +41 22 999 96 00
michele.burnier@pestalozzilaw.com