Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

The new Data Protection Act from the FDPIC's perspective

Contents

I. Introduction

The Swiss parliament passed the fully revised Federal Data Protection Act (FADP) as well as other amended pieces of legislation on data protection in its 2020 autumn session. The referendum period expired unused on 14 January 2021. The Federal Administration is currently in the process of drafting the associated implementing ordinances, which the Federal Council is expected to put into force together with the new FADP in the second half of 2022.

Until they come into effect, the private sector and federal authorities will have to adapt the processing of personal data to the new provisions. In this document, the FDPIC outlines the most important alterations that they need to take into consideration.

II. Background and objectives of the revision

The first Federal Act of 19 June 1992 on Data Protection entered into force in mid-1993 – a time when the internet was not yet used commercially and when today's digital reality, shaped by use of the ubiquitous smartphone, was still a long way off. Following a partial revision in 2008 that sought to better inform the public about how their data was processed, it quickly became clear that rapid technological developments necessitated further amendments. For the majority of the population, it is now difficult to imagine life without daily internet access and smart devices equipped with touchscreens. In order to guarantee appropriate data protection to the public, whose daily lives are shaped by cloud computing, big data, social media and the Internet of Things, a comprehensive overhaul of the FADP was inevitable.

In autumn 2017, the Federal Council approved a draft total revision of the FADP, which it referred, together with the associated dispatch, to the Federal Assembly. The aim of this revision was to adapt data protection to technological and societal changes. The new FADP must therefore meet the requirement of reinforcing citizens' rights to data protection and privacy and safeguarding them in the longer term.

Besides strengthening the rights of data subjects, in its dispatch the Federal Council highlighted the 'risk-based' approach as a guideline for the revision, according to which, the State and businesses should ascertain the risks to privacy and data protection early on, and incorporate the requirements of data protection at the planning stage of their digital projects. Major risks and the organisational and technical measures taken to mitigate them should also be documented. The revised FADP also promotes self-regulation, whereby members of sectors that issue a binding code of conduct are exonerated from certain obligations. The revised FADP also contains various new features that seek to reinforce the FDPIC's supervisory powers.

In early 2018, Parliament decided to split the revision into two parts. In order to comply with treaty implementation deadlines, initially the provisions on the processing of data were amended for federal bodies such as fedpol that apply the amended EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data in the area of criminal law, as this is part of the Schengen acquis related to the Schengen Association Agreement. This work flowed into the Schengen Data Protection Act/SDPA. The total revision of the FADP as a whole then took place in a subsequent step.

1. Stage 1: Schengen part

The SDPA entered into force on 1 March 2019. Besides the SDSG, whose term is limited until the total revision enters into force, other laws in the area of Schengen cooperation in criminal matters were then amended.

2. Stage 2: Whole FADP

In the 2019 autumn session, the National Council was the first chamber to adopt the total revision of the whole act, which the Federal Assembly then approved on 25 September 2020 once all differences had been resolved. When revising the FADP, the Federal Council and Parliament took account of the protocol amending the Convention of the Council of Europe 108[1] that has been signed by Switzerland, and the General Data Protection Regulation of the European Union (GDPR).[2] Owing to its extraterritorial scope, the latter has already been applied by large parts of the Swiss economy since it entered into force in May 2018. Despite this dependence on European law, the new FADP is in line with Switzerland's legal tradition, as it features a high level of abstraction and is technology-neutral. It sets itself apart from the GDPR not only in its brevity, but also in the sometimes different terminology it uses. In general, it is assumed that once they have updated their data protection legislation, Switzerland and the EU will mutually recognise the equivalence of their data protection levels, so that informal exchange of personal data across national borders will continue to be possible. The update to the EU Commission's equivalence decision relating to Switzerland that dates back to 2000 is expected in early 2021.

III. Most important new features of the fully-revised Data Protection Act

3. Only data of natural persons

The revised FADP only intends to protect the privacy of natural persons, about whom personal data is processed. The data of legal persons, such as commercial organisations, associations and foundations, is no longer included in the new FADP, and on this point the scope of application of the revised legislation coincides with that of the GDPR. Businesses can continue to invoke the protection of privacy provided for under Art. 28 Swiss Civil Code, the protection of manufacturing and trade secrecy as set out under Art. 162 Swiss Criminal Code, as well as the relevant provisions of federal law on unfair competition and cartels.

4. Sensitive personal data

The current definition of sensitive personal data has been extended to include genetic and biometric data provided it cannot uniquely identify a natural person.

5. Privacy by design and by default

The revised FADP enshrines the principles of privacy by design (data protection through technology design) and privacy by default (only data that is absolutely necessary to a specific purpose is processed, and this should be set out before data processing starts). These principles require authorities and businesses to implement the processing principles of the FADP from the planning stage by putting in place appropriate technical and organisational measures. Privacy by design requires that their applications and similar are designed in such a way that data is anonymised or deleted by default. Privacy by default protects users of private online offerings who have not looked into the terms of use or the associated right of objection as only the data that is absolutely necessary for the intended purpose is processed, as long as users do not take action and allow further processing. To comply with the new law, Swiss businesses need to review their offerings in a timely fashion and make adjustments where

[1] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981, ratified by the Federal Assembly on 5 June 1997. The protocol amending the Convention was approved by the Federal Assembly in summer 2020. The Federal Council will only be able to ratify it once the new FADP enters into force.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EG (General Data Protection Regulation).

necessary through the use of customer-friendly programs that are conducive to data protection.

6. Data protection officers

Under Art. 10 revFADP, businesses can designate a data protection officer who may, but does not have to be, employed by the business. In either case, advice on data protection should be separate from the business's other activities. It is also advisable not to mix advice on data protection with that of other legal advice and representation. Furthermore, data protection officers should be allowed to raise their views with company management where there are differences of opinion. Unlike in the GDPR, the designation of data protection officers for private businesses is always optional; it is only a legal requirement for federal bodies. Data protection officers are not only in-house points of contact, but also act as links to official data protection and are the first point of contact for the FDPIC. Besides providing general advice and training for employees on matters relating to data protection, their responsibilities also include involvement in the enactment and application of terms of use and data protection provisions. If the internal data protection officer is professionally independent and autonomous, and if no tasks are performed in this area that are incompatible with their role, following a data protection impact assessment, a business can refer solely to in-house advice without having to consult the FDPIC, even in cases of persistent high risk (see section 'Data protection impact assessments' below).

7. Data protection impact assessment

Data protection impact assessments are nothing new in Swiss data protection law – federal bodies are already required to conduct them. If the planned processing may involve a high risk to the privacy or the fundamental rights of data subjects, under Art. 22 revFADP, data controllers from the private sector must now also carry out a prior data protection impact assessment. The high risk comes from the nature, scope, context and purposes of processing – particularly when using new technologies. In particular, processing is deemed high risk if profiling or extensive processing of sensitive data is planned. Impact assessments of a general nature cannot absolve organisations of responsibility for recognisable risks that they fail to mention. If a product, system or service under Art. 13 revFADP is certified, or a code of conduct under Art. 11 revFADP is observed that is based on a data protection impact assessment, the drafting of a data protection impact assessment can be dispensed with. If a data protection impact assessment reveals that the planned processing still results in a high risk to the privacy or fundamental rights of data subjects, despite the measures envisaged by the data controller, under Art. 23 revFADP the data controller must obtain a prior opinion from the FDPIC. If the FDPIC objects to the impact assessment itself, it will suggest relevant clarifications or additions to the data controller. This is particularly likely if the text is formulated so generally that it fails to adequately describe the foreseeable risks or measures. If the objections are against the data processing per se, the FDPIC will propose appropriate modification measures to the controller (see also section on 'consultations'). Unlike with codes of conduct, the FDPIC's opinions do not need to be published. However, as official documents, they are subject to the Freedom of Information Act. The FDPIC consultation can be dispensed with if the internal data protection officer was consulted (see also 'Data protection officers' above).

8. Codes of conduct

Art. 11 of the new FADP provides incentives for professional, trade and business associations to develop their own codes of conduct and to submit them to the FDPIC for an opinion. The FDPIC's opinions are then published. They may contain objections and recommend relevant modifications or clarifications. Positive opinions from the FDPIC justify the legal assumption that the conduct set out in the code compiles with data protection laws. However, codes of a general nature cannot absolve organisations of responsibility for any risks that the text fails to describe in detail. By subjecting themselves to a code of conduct, members of associations

can be relieved of the task of developing their own support and guidelines for the application of the new FADP. This form of self-regulation has the advantage that data controllers do not need to conduct their own data protection impact assessment if they comply with a code of conduct that is based on a previous data protection impact assessment that is still relevant, provides for measures to protect privacy and fundamental rights, and has been approved by the FDPIC.

9. Certifications

Under Art. 13 revFADP, besides the operators of data processing systems or programs, manufacturers can also have their systems, products and services certified. Certification enables businesses among other things to provide evidence that they comply with the principle of privacy by default and that they have an appropriate data protection management system in place. If a private data controller deploys a system, product or service that is certified, they can dispense with the data protection impact assessment. The Federal Council will set out additional regulations regarding the certification procedure and quality labels in an ordinance.

10. List of processing activities

Under Art. 12 revFADP, both data controllers and data processors are now required to keep a list of all data processing activities. The new FADP sets out the minimum details. The list must always be kept up to date. In the ordinance, the Federal Council will set out exemptions for businesses with fewer than 250 employees and where data processing entails a low risk of privacy breaches for data subjects. While federal bodies are required to report the lists to the FDPIC, the new legislation no longer contains a reporting obligation for private data processors.

11. Cross-border disclosure of personal data

Under Art. 16, the revised FADP stipulates that data may be disclosed abroad if the Federal Council has ascertained that the legislation in the third country guarantees adequate protection. It will publish a list for this purpose which was compiled by the FDPIC under the previous law. If the relevant export country does not feature on the Federal Council's list, data may still be transmitted there (as under the previous law) if adequate data protection can be guaranteed by other means. This may be e.g. through international treaties, data protection clauses that must first be communicated to the FDPIC, or binding corporate rules. Standard contractual clauses that have already been approved by the European Commission under the GDPR will be recognised by the FDPIC.

If cross-border disclosure of personal data is planned - which also includes storage on foreign systems (cloud) - the countries must be indicated, regardless of whether they offer adequate data protection. In this point, the FADP goes further than the GDPR. It must also be stated which data protection guarantees, if any, are used (e.g. EU standard contractual clauses) or which exceptions according to Art. 17 revDSG, if any, the controller refers to; here, too, the FADP deviates from the GDPR.

12. Extended duties to provide information

In line with the revision's objective of promoting transparency, Art. 19 revFADP extends the duty of businesses to provide information. Under the new legislation, a private data controller must appropriately inform data subjects in advance every time personal data is collected, even if the data is not collected by them directly. In the current FADP, this duty to provide information is only stipulated for sensitive personal data and personality profiles. This means in concrete terms that the identity and contact details of the data controller, the purpose of the processing, and where applicable the recipients of personal data should be disclosed. Unlike under the GDPR, information should also be provided on the receiving state and any guarantees of an appropriate level of data protection (see above, Cross-border disclosure of personal data).

Businesses will have to review and update their privacy policies accordingly. Personal data that is only collected incidentally or along the way is exempt from the duty to provide information. The duty to provide information is restricted or waived through the many limitations and exemptions set out under Art. 20 revFADP. This is the case, for example, if data subjects already have the information, or if the processing of the data is required by law. If the data processing results in automated individual decision-making, under Art. 21 revFADP, data controllers have new duties to provide information to complainants, and to grant them the consultation and inspection rights to which they are entitled.

13. Right of data subjects to information

The right of data subjects to request information about whether data about them is being processed has been extended in the new FADP. Art. 25 revFADP contains an extended list of minimum information that data controllers must disclose, such as how long processed personal data is stored. The Article stipulates that a data subject should in general be provided with all the information that is necessary for them to assert their rights under the new FADP and to ensure transparent data processing. As in the previous legislation, the controller may refuse, restrict or defer the provision of information under certain conditions.

14. Obligation to report data security breaches

Under Art. 24 revFADP, the controller must now report data security breaches to the FDPIC if there is a high risk of adverse effects on the privacy or fundamental rights of data subjects. This provision applies both to controllers in the private sector and in federal bodies. The FDPIC should be notified of such breaches as soon as possible. Controllers should have previously drawn up a prediction of the potential implications of the breach and carried out an initial assessment as to whether there could be an imminent danger, whether data subjects need to be notified and how this could be done. If the controller does not assess the risk to be high, this does not prevent them from submitting a voluntary report to the FDPIC. Only cases involving breaches of privacy or fundamental rights have to be reported to the FDPIC, not successfully foiled or ineffective cyberattacks. The GDPR also features a reporting obligation and stipulates specific timings for incidents to be reported to EU data protection authorities. In addition, the threshold for the reporting obligation is lower under European law as it merely stipulates that the data breach must entail a risk.

15. Right to data portability

The right to data disclosure and transmission under Art. 28 revFADP means that a data subject now has the option of receiving the personal data that they have provided to a private controller in a commonly-used and machine-readable format, or having it transmitted to a third party. The conditions for this are that the controller processes the data in an automated manner and with the consent of the data subject or directly relating to a contract. This right can be exercised free of charge, except where disclosure or transmission are associated with disproportionate cost or effort. An example of the latter may be communication data where time-consuming triage is necessary to separate own statements from those of third parties.

16. Investigation of all violations of data protection regulations

The FDPIC will in future have to automatically investigate all violations of the new FADP by federal bodies or private persons (Art. 49 para.1 revFADP). In the current FADP, the restriction applies that the FDPIC only investigates cases (including clarifications of the facts) on its own initiative in cases where the methods of processing are capable of breaching the privacy of larger numbers of persons. These 'system errors' will no longer exist in future. However, as is the case under the current law, an investigation will not need to be opened for minor breaches of data protection rules (Art. 49 para. 2 revFADP). As is currently the case, the FDPIC will also

be able to dispense with formal steps if an initial contact with the data controller reveals that the deficiency to which its attention was drawn was recognised and rectified in a timely manner.

17. Authority and decisions of the FDPIC

Under Art. 51 para. 1 revFADP, the FDPIC may now conduct proceedings according to the Administrative Procedure Act[3] and formally rule against federal bodies or private data processors and controllers, adapt data processing in full or in part, suspend or even discontinue data processing, and delete personal data or have it destroyed. For example, the FDPIC can rule that a business must notify data subjects about a reported data security breach. Up to now, the FDPIC only had the authority to make recommendations and if they were not complied with, to refer the matter to the Federal Administrative Court.

An addressee may appeal against the FDPIC's decisions before the Federal Administrative Court and subsequently before the Federal Supreme Court. The FDPIC may also contest appeal decisions of the Federal Administrative Court before the Federal Supreme Court (Art. 52 para. 3 revFADP).

18. Consultations

The FDPIC is not an authorising authority or an approval body for applications, products, regulations and products. However, the new legislation sets out in various places that data controllers must consult the FDPIC before concluding relevant work and implementing their projects. For example, codes of conduct and – where there are significant residual risks – data protection impact assessments must be submitted to the FDPIC for an opinion. Given the abstract nature of these consultation matters, as a rule the FDPIC's opinions are not of a dispositive nature and do not offer any possibilities to appeal the recommended measures and requirements. If these measures and requirements remain unheeded, data controllers must assume that concrete data processing related to the FDPIC's recommendations will subsequently be the subject of decisions. These may go so far as to prohibit the data processing in its entirety, against which data controllers then have recourse to the ordinary legal remedies of administrative procedure.

19. Unprompted opinions and information for the public

Aside from the opinions published as part of formal consultation procedures, the FDPIC is still free to express unprompted opinions on new technologies, digitalisation phenomena and the processing practices of certain sectors, and to publish its opinions and assessments. In cases of general interest, the FDPIC will also inform the public – as is the case under current law – of its observations and measures. Under Art. 57 para. 2 revFADP, this also applies to observations and decisions made as part of formal investigations by the FDPIC.

20. Fees

Art. 59 revFADP regulates the services for which the FDPIC will in future charge fees to private persons. A fee is incurred for opinions on a code of conduct or data protection impact assessment, or to approve standard data protection clauses and binding corporate rules. The FDPIC will also charge private persons fees for general consulting services in future. The Federal Council will set out the details in an ordinance.

21. Sanctions

The new FADP sets out fines for private persons of up to CHF 250,000 (Art. 54 revFADP). Only intentional acts or omissions are punishable, not cases of negligence. Violation of duties to provide information and to report, and breaches of professional confidentiality are only

[3] Federal Act of 20 December 1968 on Administrative Procedure (APA), SR 172.021.

punishable on complaint. However, failure to comply with FDPIC decisions are prosecuted ex officio. In principle, the responsible natural person is fined. But companies can now also be fined up to CHF 50,000 if an investigation to determine the punishable natural person within the company or organisation would entail disproportionate effort.

As opposed to the European data protection authorities, the FDPIC is not assigned powers to impose sanctions under the new legislation. The offending persons are fined by the cantonal prosecution authorities. While the FDPIC can report an offence and enforce the rights of a private claimant in proceedings (Art. 65 Abs. 2 revFADP), it does not have the right to file a complaint. Unlike in the new FADP, the administrative sanctions under the GDPR are only applicable to legal persons. The EU data protection authorities can impose fines on offending companies of up to EUR 20 million, or 4% of annual global turnover.

FDPIC, 9 February 2021