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 approved the totally revised Federal Data Protection Act (FADP) together with other amended enactments on data protection in its 2020 autumn session. On 31 August 2022, the Federal Council decided to bring the new FADP and the associated ordinances into force on 1 September 2023.

The private sector and the federal authorities have to adapt their processing of personal data to the new provisions by the time they come into force. In this document, FDPIC would like to point out the most important changes that they must take into account.

II. Background to and objectives of the revision

The first Federal Act on Data Protection, dated 19 June 1992, came into force in mid-1993 - a time when the internet was not yet being used commercially and when today's digital reality, dominated the ubiquitous smartphone, was still a long way off. After a partial revision in 2008, the aim of which was to ensure that people would be better informed about the processing of their data, it soon became apparent that the rapid, technological advances had made further changes necessary. Today, most of the population can hardly imagine life without constantly available internet access and smart devices equipped with touchscreens. In order to guarantee the population up-to-date data protection in an everyday life characterised by cloud computing, big data, social networks and the Internet of Things, a comprehensive overhaul of the FADP became inevitable.

In autumn 2017, the Federal Council adopted the draft of a total revision of the FADP, which it submitted to the Federal Assembly with the accompanying dispatch. The aim of this revision was to adapt data protection to the changed technological and societal changes. The new FADP must thus meet the need to reinforce citizens' rights to 'informational self-determination' and privacy and to safeguard these rights in the longer term.

In addition to strengthening the rights of data subjects, in its dispatch the Federal Council highlights the 'risk-based approach' as the guiding principle of the revision, according to which the State and businesses should ascertain the risks to privacy and informational self-determination at an early stage and consider data protection requirements at the planning stage of their digital projects. Major risks and the organisational and technical measures taken to eliminate or mitigate them have to be documented. The revised DPA also encourages self-regulation by exempting members of industries that adopt a binding code of conduct from certain obligations. Lastly, the revised FADP also contains various new features that are intended to strengthen the FDPIC's supervisory powers.

In early 2018, Parliament decided to split the revision into two stages: in the first stage, the provisions on data processing applicable to federal bodies such as fedpol, which 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, were adapted in order to comply with the implementation deadlines set out in the international treaties, because they are part of the acquis to the Schengen Association Agreement. This work resulted in what is known as the Schengen Data Protection Act or SDPA. The second stage was the total revision of the FADP as a whole.

1. Stage 1: Schengen part

The SDPA came into force on 1 March 2019. In addition to the SDPA, which remains valid until the revised FADP comes into force, other laws that fall within the scope of Schengen cooperation on criminal matters were then amended.

2. Stage 2: Entire FADP

In the autumn session of 2019, the National Council as the first chamber approved the total revision of the entire Act, which the Federal Assembly then passed on 25 September 2020 after all the differences had been resolved. When drafting the new FADP, the Federal Council and Parliament took account of the protocol amending the Council of Europe Convention 108[1], which has been signed by Switzerland, as well as the European Union's General Data Protection Regulation (GDPR)[2]. Because of its extraterritorial scope, the GDPR has already been applied by many Swiss companies since it came into force in May 2018. Despite this dependence on the European law, the new FADP is in line with Swiss legal tradition as it features a high degree of abstraction and is formulated in a technologically neutral manner. It differs from the GDPR not only because of its brevity, but also because in certain cases it uses different terminology. It is generally assumed that Switzerland and the EU will mutually recognise the equivalence of their levels of data protection after revising their respective data protection legislation, so that the informal exchange of personal data across national borders will remain possible. The renewal of the EU's recognition decision towards Switzerland, which dates back to 2000, is still pending.

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

3. Only data from natural persons

The revised FADP is aimed exclusively at protecting the personality of natural persons whose personal data is processed. Data relating to legal entities, such as companies, associations or foundations, are no longer covered by the new FADP, which means that its scope of application is the same as that of the GDPR. Companies can still invoke the protection of personality under Article 28 of the Civil Code, the protection of commercial and manufacturing secrecy under Article 162 of the Criminal Code, and the relevant provisions of the federal legislation on unfair competition and cartels.

4. Sensitive personal data

The previous definition of sensitive personal data has been expanded to include genetic data and, insofar as they clearly identify a natural person, biometric data.

5. Privacy by design and by default (new: Art. 7 FADP)[3]

The revised FADP now enshrines the principles of "privacy by design" (data protection by means of technology) and "privacy by default" (data protection by means of data protection-friendly default settings). These principles require authorities and companies to implement the FADP's processing principles as early as the planning stage of projects by taking appropriate technical and organisational measures. Privacy by design requires that they design their applications in such a way that the data is anonymised or deleted by default, among other things. Privacy by default protects users of private online services who have not considered the terms of use or the rights to objection that these terms contain by ensuring that only the data that is absolutely necessary for the intended purpose is processed, as long as users do not actively authorise further processing. In order to guarantee this protection under the new law, Swiss companies should review what they are offering in a timely fashion and make

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, concluded in Strasbourg on 28 January 1981, approved by the Federal Assembly on 5 June 1997. The expansion of the Convention was approved by the Federal Assembly in summer 2020. The Federal Council will only be able to ratify it after the new FADP comes 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/EC (General Data Protection Regulation).
[3] The revised FADP is not yet available in English. This is the Link to the German version.

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

6. Data protection advisers (new: Art. 10 FADP)

Private companies may appoint a data protection adviser. This adviser may be an employee of the company, but does not have to be. In either case, the advice on data protection should be provided independently and not be influenced by other activities of the company. It is also recommended not to mix the provision of advice on data protection with that of other legal advice and representation. In addition, data protection advisers should be allowed to bring their concerns to the attention of the company management where there are differences of opinion (Art. 23 letter c Data Protection Ordinance (O-FADP)). In contrast to the European GDPR, the appointment of advisers is always optional for private entities - only federal authorities are legally required to appoint advisers. They are not only an internal contact point, but also a link to the data protection authorities and the first point of contact for the FDPIC. Besides providing general advice and training to company employees on data protection issues, their tasks include helping to draw up and apply terms of use and data protection regulations. Provided the internal data protection advisory service is professionally independent and not bound the management's instructions, and the service does not carry out any tasks that are incompatible with its responsibilities, a company can rely solely on its internal advisory service after carrying out a data protection impact assessment, even in cases of persistent high risk; the company is not required to consult the FDPIC as well (see "Data protection impact assessments" below).

7. Data protection impact assessment (new: Art. 22 et seq. FADP)

Data protection impact assessments are nothing new in Swiss data protection law - federal bodies are already required to carry them out. If a planned processing operation is likely to entail a serious risk to the data subject's personality or fundamental rights, private data controllers must now also prepare a data protection impact assessment in advance. Serious risks arise, especially when new technologies are used, from the nature, extent, circumstances and purpose of the processing. In particular, a serious risk arises from high-risk profiling or extensive processing of sensitive personal data. 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 is certified in accordance with the Data Protection Act or if a code of conduct is adhered to that is based on a data protection impact assessment, an impact assessment is not required. If it is apparent from a data protection impact assessment that the planned processing would still result in a high risk to the personality or fundamental rights of the data subjects despite the measures envisaged by the data controller, the controller must obtain the opinion of the FDPIC beforehand. If the FDPIC has objections to the impact assessment itself, he will suggest to the controller what needs to be clarified or added. This is likely to be the case primarily where the text is so general that it does not adequately describe foreseeable risks or measures. If the objections under data protection law are directed against the planned processing operations as such, the FDPIC will propose suitable ways of modifying the operations to the controller (see "Consultations" below). Unlike the codes of conduct, the FDPIC's opinions do not have to be published. As official documents, however, they are subject to the Freedom of Information Act. There is no requirement to consult the FDPIC if the internal data protection adviser has been consulted (see "Data protection advisers" above).

8. Codes of conduct (new: Art. 11 FADP)

In Article 11, the new FADP has set incentives for professional, industry and business associations to develop their own codes of conduct and submit them to the FDPIC for an opinion. His opinions will be published. They may contain objections and recommend amendments or clarifications. Positive opinions from the FDPIC establish the legal presumption that the conduct set out in the Code of Conduct complies with data protection law. However, compliance with general codes cannot provide an exemption from considering risks

that are not specified in the text. By agreeing to comply with a code of conduct, members of the associations can be absolved of having to develop their own assistance and guidelines for the application of the new FADP. This form of self-regulation also gives them the advantage that they do not have to carry out their own data protection impact assessments if they comply with a code of conduct that is based on a previous data protection impact assessment that is still up to date, that contains measures to protect the personality or fundamental rights, and that has been submitted to the FDPIC.

9. Certifications (new: Art. 13 FADP)

In addition to management systems and products, services and processes can now also be certified. Certification provides companies, for example, with evidence that they comply with the principle of privacy by default and have an appropriate data protection management system. Private data processing controllers that use a system, product or service that is certified are not required to prepare a data protection impact assessment. Further regulations on the certification procedure and quality marks have been introduced by the Federal Council by ordinance (Data Protection Certification Ordinance, in German).

10. Inventory of processing activities (new: Art. 12 FADP)

The data controller and the data processor are now each required to keep an inventory of all data processing activities. The new FADP lays down the information that the inventory must contain as a minimum. The inventory must be kept up to date at all times. In the Ordinance, the Federal Council has provided exceptions for companies that employ fewer than 250 people and whose data processing carries a low risk of violating the personality of data subjects (Art. 24 FADP). While federal bodies must submit their inventories to the FDPIC, the new law no longer provides for a reporting obligation for private entities that process data.

11. Cross-border disclosure of personal data abroad (new: Art. 16 FADP)

Under Article 16, the revised FADP stipulates that data may be disclosed abroad if the Federal Council has ascertained that the legislation in the country concerned guarantees adequate protection. The list that the FDPIC previously published is now part of the O-FADP. 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, for example, be 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 data subjects must be notified of the countries concerned, 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, if any, the controller refers to; here, too, the FADP deviates from the GDPR.

12. Extended duties to provide information (new: Art. 19 et seq. FADP)

In line with the revision's objective of promoting transparency, the new FADP extends the duty of businesses to provide information. Under the new legislation, a private data controller must appropriately inform the 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. In contrast to 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 by chance is exempt from the duty to provide information. The duty to provide information is restricted or waived through the many limitations and exemptions. 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, 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 (new: Art. 25 et seq. FADP)

The right of data subjects to request information about whether data about them is being processed has been extended in the new FADP. The new Article 25 contains an extended list of the 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 (new: Art. 24 FADP)

Under the new Article 24, the controller must now report data security breaches to the FDPIC if there is a high risk to the personality or fundamental rights of data subjects. This provision applies to controllers both 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 personality rights or fundamental rights have to be reported to the FDPIC, but 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 (new: Art. 28 FADP)

The right to data disclosure and transmission 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 the subject's own statements from those of third parties.

16. Investigation of all violations of data protection regulations (new: Art. 49 FADP)

The FDPIC will in future have to automatically investigate all violations of the new FADP by federal bodies or private persons. 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 personality rights 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. 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. Owing to its limited resources, it can generally be assumed that in handling reports even after the new Act has come into force, the FDPIC will prioritise according to the principle of discretionary prosecution.

17. Rulings (new: Art. 51 FADP)

The FDPIC may now conduct proceedings under the Administrative Procedure Act[4] 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 to the Federal Administrative Court and subsequently to the Federal Supreme Court. The FDPIC may also contest appeal decisions of the Federal Administrative Court before the Federal Supreme Court.

18. Consultations

The FDPIC is not an authorising authority nor an approval body for applications, products, regulations and projects. However, the new legislation sets out in various places that data controllers must consult the FDPIC before concluding relevant work and completing 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, the FDPIC's opinions are not normally regarded as formal rulings and do not give rise to a right of appeal against the recommended measures and requirements. If these measures and requirements remain unheeded, data controllers must assume that specific data processing covered by the FDPIC's recommendations will subsequently become the subject of formal rulings. These may even go so far as to prohibit the data processing in its entirety, in response to which data controllers will 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, without having to be requested, to express 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. This also applies to observations and decisions made as part of formal investigations by the FDPIC.

20. Fees (new: Art. 59 FADP)

The new FADP regulates the services for which the FDPIC will in future charge to private persons fees. 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 regulations. The FDPIC will also charge private persons fees for general consulting services. The details are regulated in the O-FADP (Art. 44 O-FADP).

21. Sanctions (new: Art. 50 et seq. FADP)

The new FADP sets out fines for private persons of up to CHF 250,000. Only wilful acts or omissions are offences, not cases of negligence. Violation of duties to provide information and to report, and breaches of professional confidentiality are only prosecuted on complaint.

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

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

In contrast to the European data protection authorities, the FDPIC is not assigned powers to impose sanctions under the new legislation. Offenders are fined by the cantonal prosecution authorities. While the FDPIC may report an offence and enjoy the status of a private claimant in proceedings, it does not have the right to file a criminal complaint. Unlike in the new FADP, the administrative sanctions under the GDPR are only applicable to legal entities. 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, last updated on 7 October 2022