New Swiss Data Protection Act – the most important changes for companies[1]

The new Swiss Data Protection Act (Federal Act on Data Protection - nFADP) will enter into force together with the new Ordinance to the Federal Act on Data Protection (DPO) and the new Ordinance on Data Protection Certification (DPCO) on 1 September 2023. The nFADP introduces new obligations for private persons and federal bodies, improves the rights of data subjects and significantly tightens personal criminal liability for violations of the nFADP. What do companies in Switzerland and abroad need to know to ensure data protection-compliant data processing? This article summarises the most important changes for companies.

Author
Daniela Fábián Masoch, Attorney at Law, Privacy Expert CIPP E/CIPM/FIP and ISMS 27001 Lead Auditor

FABIAN PRIVACY LEGAL
www.privacylegal.ch

Introduction

The Swiss Parliament passed the revised Data Protection Act (nFADP) on 25 September 2020.[2] The nFADP as well as the new Data Protection Ordinance (DPO) and the new Ordinance on Data Protection Certification (DPCO) will enter into force on 1 September 2023.

The aim of the revision was, on the one hand, to strengthen data protection by improving the transparency of data processing and the control options of data subjects over their data and, at the same time, to increase the sense of responsibility of those responsible.[3] Another important goal was to maintain Switzerland's competitiveness and to enable Switzerland to ratify the Council of Europe's revised data protection convention ETS 108, to align with the EU's General Data Protection Regulation (GDPR) and thus to continue to be recognized as a third country with an adequate level of data protection.

[1] *This article is an updated version of the article published in October 2020 by the same author under the same title.*
[2] *Schlussabstimmungstext DSG (final voting text in German)*
[3] *Dispatch on the Federal Act on the total revision of the Federal Act on Data Protection and the amendment of other enactments on data protection (BBl 2017 6943)*

At a Glance

- The basic concept of "permission of data processing subject to prohibition" (i.e. prohibition if the data processing leads to an "unlawful violation of the personality of a person") remains unchanged. Consent to the processing of personal data is still generally not required, even for profiling and the processing of sensitive personal data. The principles of data processing also remain largely unchanged.
- Legal entities are no longer protected; only natural persons are protected under the nFADP.
- The scope of the nFADP covers actions that have an effect in Switzerland, even if they are initiated abroad.
- The definitions of "controller of the data file", "personality profile" and "data file" have been deleted; the definitions of "profiling", "high-risk profiling" and "data security breach" have been introduced. Genetic and biometric data as well as data on ethnic origin, are considered to be sensitive personal data under the nFADP.
- The concepts of "privacy by design" and "privacy by default" are now enshrined in the law, as is already the case in the EU General Data Protection Regulation (GDPR).
- Data security is the responsibility of the controller as well as the processor. A risk-based approach is introduced.
- Data processing by processors remains largely unchanged. Under the nFADP, the processor may only assign the processing to a sub-processor with prior authorisation by the controller.
- The appointment of a data protection advisor remains voluntary. It can be an advantage when it comes to performing a data protection impact assessment.
- Under the nFADP, both the controller and the processor must keep an inventory of their processing activities. This inventory does not have to be declared to the Federal Data Protection and Information Commissioner (FDPIC) (up to now, the controller generally needed to declare data files to the FDPIC).
- Companies based outside Switzerland who process personal data of persons in Switzerland will have to designate a representative in Switzerland.
- The requirements for cross-border disclosure of personal data remain largely unchanged. Under the nFADP, the Federal Council bindingly determines whether the legislation of a state or an international body guarantees an adequate level of protection.
- The duty of information has been extended to the collection of all kinds of personal data (until now it was only applicable to the collection of sensitive personal data and personality profiles) and also includes automated individual decision-making.
- Under the nFADP, the controller must carry out a data protection impact assessment if the intended data processing may lead to a high risk for the data subject.
- In the future, the controller must notify the FDPIC of data security breaches.
- Under the nFADP, data subjects have the right to data portability.
- The powers of the FDPIC are extended. In the future, the FDPIC can order a number of administrative measures.
- The criminal provisions have been significantly tightened, with fines of up to 250 000 Swiss francs for private persons (i.e. not companies!), but only for violations in certain areas, in particular for the breach of obligations to provide access and information and to cooperate, for the violation of duties of diligence with respect to the requirements for cross-border disclosure of personal data, the appointment of a processor and for failure to comply with the minimum data security requirements.

Fines are only applicable to violations that result from a wilful act and are in most cases, only imposed upon the filing of a complaint.

The most significant changes

1. Purpose and scope[4]

The nFADP aims to protect personal privacy and the fundamental rights of natural persons whose personal data is processed. Under the current law, legal entities are also protected. By cancelling the protection of legal entities, the nFADP aligns with the GDPR, that also protects only natural persons.

The nFADP also regulates the territorial scope. According to art. 3, the law applies to actions that have an effect in Switzerland, even if they are initiated abroad.

2. Definitions[5]

Various definitions are now aligned with the GDPR.

The term "*personal data*" is limited to all information that relates to an identified or identifiable natural person. In future, only natural persons about whom personal data is processed will be considered «*data subjects*".

Concerning the identifiability, the "relative approach" is maintained. According to the *Federal Council Dispatch on the Federal Act on the complete revision of the Federal Act on Data Protection and the modification of other federal enactments*[6], the mere theoretical possibility to identify a person is, as under current law, not sufficient to presume that a person is identifiable. The Federal Council already stipulated in its Dispatch to the FADP of 1988[7] that no identifiability is given if "the effort necessary to identify a data subject is so great that, according to general life experience, it cannot be expected that any interested person should undertake such effort". "It must rather be considered what means can be reasonably employed to identify a person and be determined whether the employment of such means is reasonable under the given circumstances, for instance in terms of time and cost. In doing so, the technologies available at the time of processing and their further development must be taken into account. The law does not apply to anonymised data, if a re-identification by third parties is impossible (the data has been completely and irreversibly anonymised) or if a re-identification would only be possible with a great effort that no interested person would undertake. The same applies to pseudonymised data». [8]

The definition of "*sensitive personal data*" has been extended to include "*data on ethnic origin*", "*genetic data*" and "*biometric data which uniquely identifies a natural person*". While it is made clear that biometric data must uniquely identify a natural person, the same addition has been deleted for genetic data in the procedure of the resolution of differences.

The definitions of "controller of the data file", "personality profile" and "data file" have been deleted. The following new definitions have been introduced:

[4] *Art. 1-4 nFADP*
[5] *Art. 5 nFADP*
[6] *BBl 2017 7019*
[7] *BBl 1988 II 444*
[8] *BBl 2017 7019 (translated from the German text)*

- "*controller*": a private person or federal body that alone or jointly with others decides on the purpose and the means of the processing.
- "p*rocessor*": a private person or federal body that processes personal data on behalf of the controller.
- "*profiling*": any form of automated processing of personal data consisting in the use of such data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, whereabouts or movements.
- "*high-risk profiling*": profiling which involves a high risk to the personality or fundamental rights of the data subject, by creating a link between data which allows an assessment of substantial aspects of the personality of a natural person.
- "*data security breach*": a security breach which leads to an unintentional or unlawful loss, deletion, destruction or modification of personal data or to personal data being disclosed or made accessible to unauthorised persons.

3. Principles of data processing

The principles of data processing remain materially largely unchanged.

- Art. 6 para. 4 now explicitly stipulates that personal data must be destroyed or anonymised as soon as it is no longer needed with regard to the purpose of the processing. To comply with this obligation, the controller must determine retention periods in advance.
- The definition of "personality profile" is replaced by "profiling" (see description under "definitions"). The terminology of profiling was the sticking point on which the Councils disagreed until the very end and which was also largely discussed in the media. In the end, the conciliation committee followed the proposal of the Council of States and decided to introduce the definition of "high-risk profiling" (which is comparable to the current concept of the personality profile), with the consequence that if consent is required for this type of profiling, it must be explicit.

It should be noted that the nFADP does not introduce a consent requirement for high-risk profiling, but only requires that consent, if at all required as a justification under art. 31 nFADP, must be given explicitly. It is worth recalling that the basic concept of both the FADP and the nFADP is different from that of the GDPR. While under the GDPR, a legal ground is always required for the processing of personal data (art. 6 and 9 GDPR), the processing of personal data under the FADP and nFADP is, in principle, permitted as long as the personality of the data subjects is not unlawfully violated. Hence, the "permission principle subject to prohibition" continues to apply under the nFADP, while the GDPR applies the "prohibition principle subject to permission".

4. Privacy by Design und Privacy by Default

The principles of "*privacy by design*" and "*privacy by default*", as known from the GDPR, are now also enshrined in the nFADP. In today's practice, the controller is already required to set up data processing activities in a manner that complies with the data protection regulations and the principles of data processing. The nFADP explicitly regulates that the controller must ensure, through appropriate pre-defined settings, that the processing of personal data is limited to the minimum required by the purpose unless the data subject determines otherwise (privacy by default).

You can read more about the concept in my article Privacy by Design as a Fundamental Requirement for the Processing of Personal Data.

5. Data security

The slightly revised article 8 nFADP stipulates that both the controller and the processor must ensure, through adequate technical and organisational measures, a level of data security that appropriately addresses the risk. This means that a risk-based approach is introduced. "The higher the risk of a data security breach, the higher the requirements for the measures to be taken".[9] Further provisions on minimum data security requirements can be found in Section 1 of the DPO.

6. Data processing by processors

Art. 9 nFADP essentially adopts the current article 10a FADP. The rather unfortunate term "third parties" is replaced by "*processors*". The processing of personal data may still be assigned by agreement or by legislation to a processor if (a) the data is processed only in a manner permitted for the controller itself, and (b) no statutory or contractual duty of confidentiality prohibits the assignment. The controller must ensure in particular that the processor can guarantee data security. As under the GDPR, the processor may only assign the processing to a sub-processor with the prior authorisation by the controller.

7. Data protection advisor

Controllers may, but are not required to, appoint a data protection advisor as a contact point for the data subjects and the relevant authorities responsible for data protection matters in Switzerland. The data protection advisor has the duty to train and advise the controller in matters of data protection and to participate in the enforcement of data protection regulations.

Contrary to the current FADP, the data protection advisor is not responsible for supervising the company's internal compliance with data protection regulations, nor for maintaining an inventory of data files.

Private controllers who appointed a data protection advisor have an advantage when they need to perform a data protection impact assessment according to art. 22 nFADP by reason of their processing activities, provided that they consult their data protection advisor. In this case, they can abstain from consulting the FDPIC.[10] The controller must consult the FDPIC before the processing when 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 may abstain from consulting the FDPIC if the data protection advisor (a) performs his or her function towards the controller in a professionally independent manner and without being bound by instructions, (b) does not perform any activities which are incompatible with his or her tasks as data protection advisor, (c) possesses the necessary professional knowledge, and (d) if the controller publishes the contact details of the data protection advisor and communicates them to the FDPIC.

[9] *BBl 2017 7031*
[10] *Art. 23 para. 4 nFADP*

8. Inventory of processing activities

As under the GDPR, controllers and processors must each keep an inventory of their processing activities. The nFADP lists the minimum information that needs to be contained in such inventories. The inventory of processing activities does no longer have to be declared to the FDPIC.

9. Representative in Switzerland

Similar to the GDPR, private controllers with their domicile or residence abroad must, under certain circumstances, designate a representative in Switzerland if they process personal data of persons in Switzerland. The representative serves as a contact point for data subjects and the FDPIC. The controller must publish the name and address of the representative. The requirements for designating a representative and the duties of the representative are regulated in art. 14 and 15 nFADP.

10. Cross-border disclosure of personal data

Under the current FADP, personal data must not be disclosed cross-border if such disclosure would seriously endanger the personal privacy of the data subjects, in particular, due to the absence of legislation that guarantees adequate protection. The FDPIC maintains a list with a general evaluation of the data protection level in the listed countries. However, this non-binding list does not relieve the data exporter from its responsibility to assess on a case by case basis whether the legislation of the respective country guarantees an adequate level of protection.

Under the nFADP, the Federal Council bindingly determines whether the legislation of a state or an international body guarantees an adequate level of protection. If this is the case, personal data may be transferred cross-border. If not, data protection must be guaranteed by measures such as (a) an international treaty, (b) data protection clauses between the contracting parties, which were communicated beforehand to the FDPIC, (c) standard data protection clauses previously approved, established or recognised by the FDPIC (such as the EU standard contractual clauses) or (d) binding corporate rules (BCR) previously approved by the FDPIC or by a foreign authority which is responsible for data protection and belongs to a state which guarantees adequate protection (for example the CNIL in France as lead authority). The Federal Council can provide for other adequate safeguards, such as, for example, a follow-up agreement to the Swiss-US Privacy Shield.[11]

By derogation from the principles mentioned above, personal data may only be disclosed cross-border if one of the exceptions provided for in art. 17 nFADP applies, such as, for example, the explicit consent of the data subject.

11. Duty of information when collecting personal data

The duty of information has been tightened. While the duty of information currently only applies to the collection of sensitive personal data and personality profiles, the controller must, in the future, generally inform the data subjects about the collection of their personal data. The minimum information that must be

[11] *On 8 September 2020, the Federal Data Protection and Information Commissioner (FDPIC) determined that the Swiss-US Privacy Shield was no longer adequate for the transfer of personal data from Switzerland to the US. The European Commission and the United States announced in March 2022 an "agreement in principle" on the new Transatlantic Data Protection Framework (TADPF), which is intended to facilitate the flow of data between the EU and the US and address the concerns raised by the European Court of Justice in the Schrems II decision in 2020. US President Biden subsequently issued the Executive Order On Enhancing Safeguards for United States Signals Intelligence Activities in October 2022, implementing US commitments under the TADPF. On 13 December 2022, the European Commission published a draft adequacy decision concluding that the EU-US data protection framework provides an adequate level of protection for personal data transferred by EU companies to the US. A final decision by the European Commission is expected around mid-2023.*

given in the privacy statement is stipulated in art. 19 nFADP, differentiating between data collected directly from the data subject and data collected indirectly via other sources. This minimum information is less extensive than under the GDPR. However, there is one aspect where the nFADP is stricter than the GDPR: if personal data is disclosed cross-border, the controller must inform the data subject of the state where the recipient is located, no matter whether it is located in a state with an adequate level of data protection or in a third country.

Exceptions to the duty of information have been concretised. Private controllers may still restrict, defer or waive the provision of information in some instances. Among others, this is possible when the overriding interests of the controller demand it and when the controller does not disclose the personal data to third parties, companies controlled by the same legal entity not being considered as third parties in the sense of this exception.

Under the nFADP, the controller must, as a general rule, inform the data subject of a decision which is taken exclusively based on automated processing and which has legal effects on the data subject or affects him or her significantly (so-called "automated individual decision"). The data subject can request that a natural person review the automated individual decision. Art. 21 nFADP provides for exceptions to this rule.

12. Data protection impact assessments

As under the GDPR, the controller must conduct a data protection impact assessment before the data processing if the intended data processing may lead to a high risk for the data subject's personality or fundamental rights. The existence of high risk, particularly when using new technologies, depends on the nature, the extent, the circumstances and the purpose of the processing (in particular the processing of sensitive personal data on a broad scale and the systematic surveillance of extensive public areas).

The data protection impact assessment contains a description of the intended processing, an evaluation of the risks for the data subject's personality or fundamental rights, as well as the intended measures to protect the data subjects' personality and fundamental rights. Art. 22 nFADP provides for certain exceptions. If the controller considers performing several similar processing operations, it may establish a joint impact assessment.

If the data protection impact assessment shows that the intended processing leads to a high risk for the personality or the fundamental rights of the data subject despite the measures envisaged, the controller must consult the FDPIC before the processing. It can abstain from consulting the FDPIC if it has appointed a data protection advisor according to art. 10 nFADP and consulted him or her regarding the processing in question.

13. Notification of data security breaches

Like the GDPR, the nFADP introduces a duty of notification of data security breaches, i.e. security breaches that lead to the unintentional or unlawful loss, deletion, destruction or modification of personal data or to personal data being disclosed or made accessible to unauthorised persons.

The good news is that the provisions regarding the notification obligation are slightly more pragmatic under the nFADP than under the GDPR. 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 or the fundamental rights of the data subject.

Unlike the GDPR, the nFADP only requires notification to the FDPIC where there is a *high* risk for the data subject. This is meant to prevent the notification of minor breaches. It remains the responsibility of the controller to determine the impact of the breach and the resulting risk for the data subject.

Contrary to the GDPR, the nFADP does not stipulate a specific period within which the notification to the FDPIC must be made, but demands that the controller notify the breach *as soon as possible* after having become aware of it. The controller must act quickly but has a certain margin of discretion. "What is decisive in this context is, among others, the extent of the threat for the data subject. The bigger the threat and the larger the number of data subjects concerned, the quicker the controller must act."[12] Furthermore, the controller only needs to inform the data subject if it is necessary for the protection of the data subject or if the FDPIC requests so. What is decisive in this context is whether the notification can reduce the risk for the personality or the fundamental rights of the data subject. This is, in particular, the case where the data subject can take measures for his or her protection, for example by changing his or her login details or password. [13] Under certain circumstances, the controller may restrict the information to the data subject, defer it or refrain from providing information.

The processor has no duty to notify the FDPIC but must inform the controller as soon as possible of any data security breach.

Art. 24 nFADP lists the minimum requirements for a notification to the FDPIC.

14. Rights of the data subject

Access right: The access right currently regulated in art. 8 FADP is now regulated in art. 25 nFADP. The principle remains unchanged. The controller provides the data subject with the information required to enable him or her to assert his or her rights and to ensure the transparent processing of personal data. It is the same information as the one that must be given based on the duty of information. The minimum information that must be provided in reply to a request for information is listed in the nFADP. A new element is information on the existence of automated individual decision-making. In this case, the data subject must also be informed about the logic on which the decision is based. The data subject can further request that a natural person review the automated individual decision.

The current limitations to the access right continue to exist. Under the nFADP, the controller may "refuse, restrict or defer the provision of information if the request for information is manifestly unfounded or is obviously of a querulous nature". According to the Federal Council Dispatch [14], this limitation is to be interpreted in a narrow sense. In particular, the controller must choose the most favourable solution for the data subject. It must, to the extent possible, only restrict the provision of information, may defer it if necessary and can only refuse it in absolutely clear and obvious cases.

Right to data portability: Under the nFADP, the data subject has, under certain circumstances, a right to data portability.[15] The data subject may request the transfer of his or her personal data to him or her or, if this does not involve a disproportionate effort, to another controller. As a general rule, the data must be disclosed free of charge and in a standard electronic format. The same limitations as for the access right apply.

[12] BBl 2017 7064
[13] BBl 2017 7065
[14] BBl 2017 7069
[15] Art. 28 nFADP

Legal claims: The currently applicable legal claims continue to apply and are listed in art. 32 nFADP. The right to deletion or destruction is now explicitly regulated in the nFADP, although it is already implied in the current law.

15. Administrative measures and sanctions

The competences of the FDPIC are extended in art. 51 nFADP. Under the new law, he can not only recommend measures but also order administrative measures. Among these measures are for example measures against data processing that violates the data protection regulations, including the order to destroy personal data or the prohibition to disclose personal data cross-border, as well as the order to perform a data protection impact assessment or to inform the data subject. The FDPIC still cannot issue any fines. This competence remains with the cantons.[16]

The criminal provisions have been significantly tightened.[17] Under the nFADP, private persons (i.e. not companies, as under the GDPR!) are, on complaint, liable to a fine of up to 250 000 Swiss francs if they violate their duty to provide access or information, or their duties of diligence, namely if they disclose personal data cross-border or assign the data processing to a processor without complying with the requirements, or fail to comply with the minimum data security requirements. Persons who wilfully refuse to cooperate with the FDPIC in the context of an investigation are also liable to a fine.

Further, a person who violates his or her duty of confidentiality by wilfully disclosing secret personal data of which he or she has gained knowledge while exercising his or her profession which requires knowledge of such data is liable to a fine. This provision introduces a duty of confidentiality for persons (and their auxiliary persons) who are not covered by the obligation of professional secrecy under criminal law [18]. A breach of professional confidentiality can be sanctioned on a complaint with a fine of up to 250 000 Swiss francs.

Finally, persons who wilfully fail to comply with a decision issued by the FDPIC or by the appellate authorities under threat of penalty are liable to a fine of up to 250 000 Swiss francs.

It should be noted that only those who act intentionally are liable to prosecution, whereby contingent intent is sufficient. The addressees of the penal provisions are in principle managers, i.e. persons who have independent decision-making powers.[19] The company can only be directly fined if the fine does not exceed 50 000 Swiss francs and the investigation of the culpable manager would require disproportionate investigative measures.[20]

Finally, it should be noted that violations of essential duties newly enshrined in the law, such as the keeping of an inventory of processing activities, the notification of data security breaches or the obligation to perform data protection impact assessments, are not liable to a fine.

[16] *Art. 65 nFADP*
[17] *Art. 60ff. nFADP*
[18] *Art. 321 Swiss Criminal Code (StGB)*
[19] *BBl 2017 7099, Art. 29 StGB, Art. 6 VStrR*
[20] *Art. 7 VStrR*

Implementation measures

Companies should carry out a data management analysis and identify their level of compliance with the nFADP as well as any possible gaps and risks. In doing so, they should focus on the following areas:

- governance structure,
- data protection standards and processes to comply with the privacy principles and data security,
- transparency towards the data subjects,
- inventory of processing activities,
- data flows within the company and to service providers (taking into consideration the latest developments and the policy paper of the FDPIC[21]),
- processes for performing data protection impact assessments,
- notification of data security breaches to the FDPIC and
- responding to requests for information (access rights).

Companies who already introduced a GDPR data protection program will have less need for action than companies who are not subject to the GDPR or who have not yet taken any respective measures.

Many companies will, in any case, have to introduce concepts such as privacy by design as well as processes that allow the legally compliant deletion or destruction of personal data and support data portability. Many companies will also have to review their privacy statements and, if needed, adapt them or issue new privacy statements to fulfil the requirements of the nFADP. Current inventories of data files will have to be restructured to record data processing activities.

If you have any questions or need support in this area, please do not hesitate to contact FABIAN PRIVACY LEGAL.

[21] *Policy paper of the FDPIC*