Revision of the Swiss Federal Act on Data Protection: The countdown for Swiss companies runs

May 2023

Contents

About the Authors

Dr Dirk Spacek, LL.M.
Partner | CMS Switzerland
T +41 44 285 11 11
M +41 79 696 20 46
E dirk.spacek@cms-vep.com

Julia C. Nitschke
Associate | CMS Switzerland
T +41 44 285 11 11
M +41 79 655 92 93
E julia.nitschke@cms-vep.com

Dirk Spacek is in charge of the practice groups TMC, Data Privacy and IP. He primarily deals with new business models and methods of data commercialization arising in the media-, internet- and technology-sector as well as intellectual property law.

Dirk Spacek mainly advises clients from the media, software, life sciences and financial services-sectors on technology-related matters, in particular IT-contract law, cloud computing, outsourcing, data protection, cross-border-data management projects, data cybersecurity and intellectual property law. In data privacy matters, Dirk often advises on strategic and cross-jurisdictional implementation of data storage and processing matters.

Julia Nitschke's practice focuses primarily on arbitration and litigation as well as advising clients in all aspects of civil and commercial law matters. She is part of the practice groups TMC and IP and advises clients especially from the media, software, life sciences and financial services industries on technology-related matters, in particular in the areas of data protection, IT contract law, outsourcing, cybersecurity and intellectual property law with a focus on copyright and patent law.

Introduction

What happened? Where do we stand?

After the two chambers of Swiss parliament reached consensus on the revision of the Swiss Federal Act on Data Protection ("**new Federal Act on Data Protection**" or "**nFADP**"; current Federal Act on Data Protection of 19 June 1992 "**FADP**"), on 31 August 2022, the Federal Council decided that the nFADP as well as the implementing provisions in the new Data Protection Ordinance ("**nDPO**") and the new Ordinance on Data Protection Certifications ("**nDPCO**") is scheduled to enter into force on 1 September 2023.

Given the entry into force of the EU General Data Protection Regulation ("**GDPR**") in May 2018, one of the purposes of the total revision of the FADP is to harmonize with the latest developments in the European Union, but at the same time to maintain its local particularities, especially the more liberal approach than under the GDPR. The revision of course aims at continuing to maintain a positive adequacy decision by the EU Commission. With the nFADP, Switzerland will take a similar step than the European Union, but still maintains a considerably more liberal approach. Furthermore, it is partially providing for even stricter requirements than the GDPR (e.g. location of data must be disclosed in data privacy policies with sufficient degree of precision).

The revision of the FADP aims at

(i) improving the transparency of data processing,
(ii) strengthening the data subject's protection of personal data and their control, and
(iii) enhancing the supervision system of the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

Besides this, the nFADP will introduce a new sanctions regime. In the event of a breach of obligations to provide access and information or to cooperate, fines of up to 250,000 Swiss Francs will be threatened, which will not (as in the GDPR, for example) be designed as an administrative penalty, but will be imposed as a criminal sanction on the responsible individuals involved within a company (Art. 60 to 64 nFADP). For comparison: The current FADP provides for criminal fines only up to 10,000 Swiss Francs for breaches of a limited number of obligations (Art. 34 FADP, Art. 106 para. 1 Swiss Criminal Code).

In exceptional cases of violations committed within companies, sanctioned with a fine not exceeding 50,000 Swiss Francs, the competent authority may sentence the company directly to the payment of the fine if it would be disproportionately cumbersome to detect the individuals responsible due to e.g. organization flaws (Art. 64 nFADP).

In addition, there are also a number of (presumably) less decisive changes for operating businesses: For example, personal data pertaining to legal entities (such as commercial companies, associations or foundations) will no longer be covered by the nFADP which brings the scope of the nFADP in line with the GDPR and most foreign data protection laws. With the entry into force of the nFADP, "personal data" is henceforth defined as information relating to an identified or identifiable natural person (art. 5 let. a nFADP). Information relating to legal entities is no longer defined as "personal data" as this is the case under the current FADP.

There is no grace period in the sense of a transition period for applicability of the nFADP. Nevertheless, the early announcement by the government has given Swiss companies sufficient time to implement necessary adjustments in their data protection management.

Unlike what many people predicted, the essential pillars of the current FADP will remain in place (in particular the more liberal approach embodied in Swiss data protection law based on the principle of informational self-determination). Switzerland will not adopt a "copy" of the GDPR, but merely adopt what seemed reasonable, i.e. compatible with the prior established data protection principles in Switzerland. Consequently, the private sector in Switzerland will not have to fundamentally change the way it has processed personal data in the past. One significant difference is that under the nFADP, data processing activities will not be considered forbidden in general and subject to justification grounds. Instead, data processing activities will be considered permitted as long as the established data processing principles are complied with. Only in the event of infringements of these principles, justification grounds will be necessary to invoke under the nFADP (as under the old FADP).

The nFADP provides for the following most important revision features:

— Section 1:
Extended information obligations (e.g. explicit obligation for data privacy policies)
— Section 2:
Extended documentation obligations (e.g. records of data processing activities)
— Section 3:
Extended governance rules:
3.1. Conduct of Data Privacy Impact Assessments (DPIAs)
3.2. Data breach notifications
3.3. (Voluntary) appointment of a Data Protection Advisor
3.4. Designation of a Swiss representative
— Section 4:
Data processing activities by third parties and cross-border transfers
— Section 5:
More comprehensive data security obligations (Privacy by Design and Privacy by Default)

Section 1: Extended information obligations

1.1. General information duties of the controller

The revision of the FADP aims to improve transparency in data processing and to strengthen the rights of data subjects. While the information obligations under the current FADP have been regulated in a more implied manner, the nFADP stipulates expressly the obligation to provide all necessary information on data processing to the data subjects.

According to Art. 19 nFADP, the controller must inform the data subject appropriately about the collection of personal data, in particular about

- the controller's identity and contact information,
- the purpose(s) of processing,
- (in case of disclosure to third parties) the (categories of) recipients,
- (in case of data not collected from the data subject itself) the categories of personal data, and
- (in case of cross-border disclosure) the name of the State or international body and, as the case may be, the safeguards.

It is recommended to choose a form that meets the purpose of transparent data processing and to ensure that the data subject actually has the opportunity to take note of the information. If the information is provided in combination with pictograms that are displayed electronically (i.e. privacy icons), it is recommended that these pictograms should be machine-readable.

Compared to the current FADP, the special information duties for the data collections of sensitive personal data and personality profiles will be abolished. Information duties to data subjects will be understood to apply in a general fashion and not only for particular data collections.

Compared to the GDPR, Art. 13 GDPR provides more extensive obligations regarding the information to be provided. However, the provision of Art. 19 nFADP will insofar be stricter as the GDPR as every location of data storage must be explicitly mentioned. Scholars are currently of the view that regional indications should suffice (e.g. "in the EU").

The nFADP provides for strict deadlines for the fulfilment of the information obligations: If the personal data is obtained from the data subject himself, the data subject must be informed *"when the information is obtained"* (Art. 19 para. 2 nFADP). If the personal data is not obtained from the data subject himself, the data subject should be informed about the data collection proactively (e.g. in a suitable general form or by individual information) at the latest one month after receiving of the personal data, or (if applicable) already earlier at the time of disclosure.

1.2 Information obligation for automated individual decision-making

In view of technological developments and similar to Art. 22 GDPR, the Swiss legislator will introduce an information obligation for automated individual decision-makings (Art. 21 nFADP). An automated individual decision is one based exclusively on automated processing, i.e., when no substantive

evaluation (and decision based on it) has been made by a person (especially in the case of profiling, automated tax assessments, AI-based rejection of a job application, credit scoring that leads to the non-conclusion of a credit agreement or its termination). With the entry into force of the nFADP, a controller will have to provide the data subject an opportunity to express his or her point of view, if requested. Other than under the GDPR, an individual may also waive his right to information and human re-assessment of an automated decision. In particular, the rights of Art. 21 nFADP may not be invoked if the automated decision taken was the one already chosen/applied for by the individual earlier (e.g. an applied bank credit is granted based on an automated decision or an online-transaction is executed based on the individual's wish/request; see Art. 21 para. 3 nFADP).

According to Art. 60 para. 1 nFADP, private persons will be liable to a fine of up to 250,000 Swiss Francs if they breach their obligations under Art. 19 and Art. 21 nFADP by wilfully providing false or incomplete information or by wilfully failing to inform the data subject.

1.3 Data Subject Access Requests

The newly regulated right of access in Art. 25 nFADP will contain a list of information that must be provided to data subjects upon request in case they exercise a Data Subject Access Request ("**DSAR**"). The current provision for DSARs (Art. 8 FADP) is more or less similarly shaped as the new one with the exception that Art. 25 nFADP will provide a slightly wider catalogue of data which must be provided to the requesting data subjects:

— identity and contact details of the controller;
— the personal data being processed as such;
— the purpose of processing;
— the period of storage of the personal data or, if this is not possible, the criteria used to determine such period;
— the available information on the origin of the personal data, to the extent that it was not collected from the data subject;
— if applicable, the existence of an automated individual decision as well as the logic on which this decision is based;
— if applicable, the recipients or categories of recipients to which the personal data was disclosed as well as (in case of cross-border data transfers) the information foreseen in Art. 19 para. 4 nFADP (name of the state or international body and, as the case may be, safeguards).

The list should cover all information, which the controller must provide to the data subject. However, the list is not exhaustive. Subsidiarily, the general clause in Art. 25 para. 2 nFADP will allow to request further information, if this is required for the data subject to assert his rights and/or to ensure transparent data processing. As already mentioned under the current FADP, the controller must provide the information free of charge (Art. 25 para. 6 nFADP). Exceptions to the obligation to provide information free of charge will be limited to cases where providing the information would involve disproportionate effort or the controller provides for a more standardized cost clarification procedure (Art. 19 nDPO).

A substantive chance to the current FADP should be seen in the fact that wilful provisions of false or incomplete answers to a DSAR will now be subject to criminal sanctions (Art. 60 para. 1 let. a nFADP). Often in practice requested so called "declarations of completeness" should preferably not be signed.

1.4 Data portability

The nFADP will stipulate a right to data portability (28 nFADP). Data portability was not envisaged in the initial Federal Council's revision proposal; it was only proposed later, in parliament and can be considered as a result of "political lobbying". To a certain degree, this provision bears similarities with Art. 20 GDPR according to which any person may request from the controller, free of charge, the disclosure of the personal data that he has disclosed to him in a standard electronic format if a) the controller processes the data in an automated manner, and b) the data is processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject. In addition, if this does not involve a disproportionate effort, the data subject may request the controller to transfer his personal data to another controller. Ultimately, the goal of the Swiss "data portability" provision is to confer a termination assistance right to individuals to have their data migrated in a commonly usable electronic form to a successor provider.

Key points:
Extended information obligations

The newly imposed information obligations under the nFADP will expressly provide in the wording of the statute and non-compliance will be sanctioned with criminal fines up to 250,000 Swiss Francs (imposed on individuals working within the relevant company).

Although these provisions are not as "new" as they seem on the surface (most professionally organized Swiss companies have already deployed privacy policies on their website in the past; the current Art. 4 FADP already establishes the general notion that data processing activities and their purposes must be "evident" to a data subject "at the time of collection"), Art. 19 nFADP will enshrine this principle expressly, in a more detailed and standardized manner.

In distinction to the GDPR, the catalogue of necessary information is not formulated in an exhaustive manner (see the formulation "in particular"). In the case of cross-border data transfers, the nFADP requires that all locations where personal data is stored are disclosed. This is slightly stricter than under the regime of the GDPR.

Suggested measures:

- Review of privacy policies (esp. regarding extended information obligations and Swiss particularities);
- Establishment of processes with regard to automated decisions conducted within an organization and legal information to be provided to data subjects;
- Establishment of processes with regard to Data Subject Access Requests (DSARs) and the answering procedure;
- Training of personnel on revised data protection matters and their supervision within a company (training of DPOs or individuals responsible for data protection).

Section 2: Extended documentation obligations

Under the nFADP, controllers and processors will have to maintain records of data processing activities ("RPAs") handled under their respective responsibility (Art. 12 nFADP). With the exception of Federal governmental bodies (Art. 12 para. 4 nFADP), this documentation duty will replace the former duty to notify data files to (and to register them with) the FDPIC (see Art. 11a para. 2 FADP).

The obligation to maintain RPAs is a considerable change and will cause additional efforts for Swiss companies with lower amounts of staff. Nevertheless, the obligation to maintain RPAs will not per se be sanctioned, but only "indirectly" punishable: E.g. if the controller or the processor wilfully refuses to cooperate with the FDPIC, he can be liable to a fine up to 250,000 Swiss Francs (Art. 60 para. 2 nFADP). Under the GDPR, the violation of the obligation to keep RPAs is "directly" subject to a fine under Art. 83 para. 4 let. a GDPR.

While the information duties (see Section 1) purport to inform individuals outside, the documentation duties aim at gaining internal clarity over the most relevant data processing activities within a company. RPAs constitute a general description of the processing activities, i.e. a written presentation of the essential information (in particular the type and scope) on all data processing activities. It is not necessary to keep a "protocol" of all individual actions of the controller or processor since the RPA is only intended to draw significant conclusions on whether a data processing operation complies with general data protection principles or not.

RPAs are not intended to be disclosed to a data subject. Only, in cases of investigations of breaches of data protection regulations, should the controller or the processor not comply with the duty to cooperate with the FDPIC, the FDPIC may demand access to RPAs to the extent required for his investigations (Art. 50 para. 1 let. a nFADP).

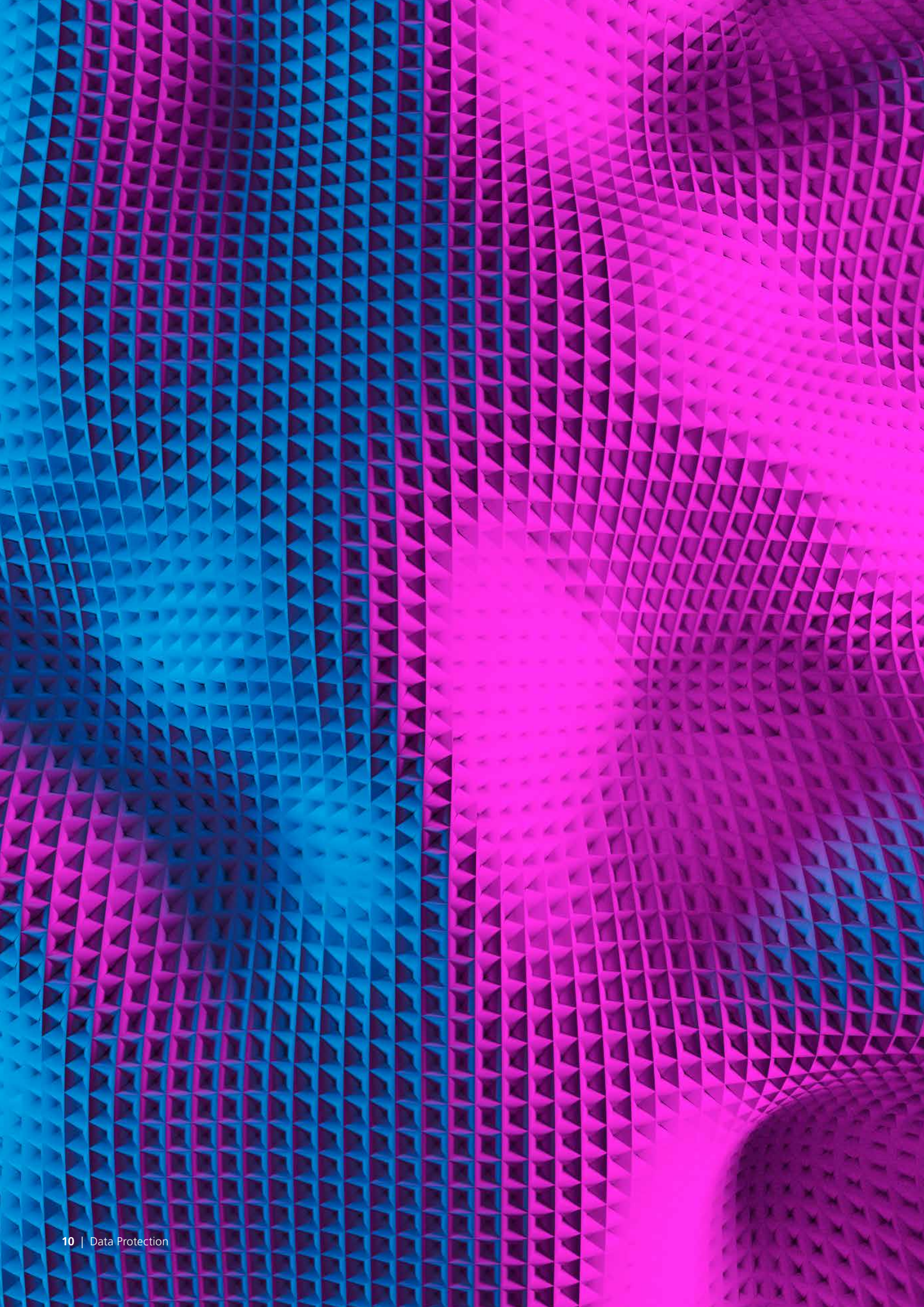
Even though the establishment of RPAs is advisable in many cases, the Swiss legislator allows for an exemption. In order to relieve small and medium-sized companies, exemptions will apply to companies with less than 250 members of staff for data processing activities only associated with low risks of infringing the personality of data subjects (Art. 12 para. 5 nFADP).

Key points:
Extended documentation obligations

Upon entry into force of the nFADP, generally speaking, the controllers and the processors will have to maintain records of the essential information on all data processing activities. This extended documentation obligation will replace the former duty to notify data files to the FDPIC. Companies that already maintain RPAs under Art. 30 GDPR should be in line with this new obligation. Even if, under certain conditions, this obligation will not apply to companies with less than 250 members of staff, RPAs can still be useful, since they provide a quick overview on all data privacy management activities and help to diagnose and establish any further necessary data protection measures.

Suggested measures:

— Preparation and maintenance of RPAs, if not yet existing and required.



Section 3: Extended governance rules

3.1. Conduct of Data Privacy Impact Assessments (DPIAs)

The nFADP will introduce a new obligation to conduct DPIAs and, thus, follows the similarly enacted European requirements of Art. 35 GDPR. According to Art. 22 para. 1 nFADP, a controller is obliged to conduct DPIAs beforehand, if the intended data processing may lead to a high risk for the data subject's personality or fundamental rights, all of which is depending on the nature and the extent of the processing as well as the circumstances and the purposes of processing (e.g. sensitive personal data on a broad scale and systematic surveillance of extensive public areas would be considered to involve potential high risks).

The nFADP does not specify under which process a DPIA must be conducted but it allows the controllers to introduce a framework, which complements their existing working practices provided it takes into account the following minimum requirements for DPIAs described in Art. 22 para. 3 nFADP:

— a description of the intended processing *(Which data is processed by whom, for what purpose, how and where and, if necessary, passed on?),*
— an evaluation of the risks as regards the data subject's personality rights *(With a certain probability, what negative physical, immaterial or material consequences could the data processing have for the data subject?),* as well as
— the intended measures to protect the data subject's personality or fundamental rights.

DPIAs are self-assessments under data protection law. Companies will have the possibility to abstain from establishing a DPIA if they have been certified in accordance with Art. 13 nFADP or if they comply with a code of conduct in accordance with Art. 11 nFADP, which meets the requirements set forth in Art. 22 para. 5 nFADP. Needless to say that these certification must relate to the processing activities in question under the DPIA.

If the DPIA 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 company will be obliged to submit the results to and consult the FDPIC prior to starting with the processing activities (Art. 23 nFADP). According to Art. 23 para. 4 nFADP, a company may omit to consult the FDPIC if he has consulted his own appointed data protection advisor according to Art. 10 nFADP (for further information on the data protection advisor, see later). Under the GDPR, also processors are mandatorily required to assist controllers in the conduction of DPIAS (see Art. 28 para. 3 let. f GDPR). Nevertheless, in Switzerland, controllers and processors regularly conclude data processing agreements, which in practice often include such same clauses to support controllers with conducting DPIAs.

Art. 69 nFADP formally provides a transitional period for DPIAs on data processing operations that were started before 1 September 2023. However, this transitional period is limited to cases where the purpose of processing remains unchanged after such date and no new data is included in the data processing activities. This is rarely the case and therefore practically less relevant.

Key point:
Conduction of DPIA

With the entry into force of the nFADP, the Swiss legislator introduces the obligation to conduct DPIAs. DPIAs as self-assessments under data protection laws to evaluate risks for the data subject's personality rights if processing involves a high risk for the personality or the freedom of the affected individuals. Compared to the GDPR, the nFADP is less onerous in that no prior consultation of the FDPIC is necessary, if the controller has appointed his own data protection advisor.

Suggested measures:

— If necessary and required (i.e. processing activities bear high risks for the personality or the freedom of affected individuals): Periodical conduct of DPIAs.

3.2. Data breach notifications

The current FADP does not provide for mandatory notification obligations to supervisory authorities in case of data protection violations. Thus, it deviated substantially from the GDPR-standard. Nonetheless, even under the current FADP, the principle that the processing of personal data must be carried out in good faith (Art. 4 para. 2 FADP) may imply that data security breaches should sometimes be notified, at least to the data subjects. Notification obligations to data subjects may also arise from other statutory bases (e.g. contractual diligence obligations of an agent towards the principal).

With the entry into force of the nFADP, the Swiss legislator has explicitly established data breach notification obligations: According to Art. 24 para 1 and para. 3 nFADP, a controller must henceforth report data breaches to the FDPIC *"as soon as possible"* and the processor must henceforth report the same *"as soon as possible"* to the controller. Notice must indicate the data security breach, its consequences and the measures taken or foreseen. Cases in which a data security breach has occurred include, in particular, the loss, destruction, modification or disclosure of personal data to unauthorized persons. Insignificant breaches, i.e. those that are not probable to result in a *high risk* to the personality or fundamental rights of the data subject, do not have to be reported. This constitutes a significant difference to the GDPR under which data breaches, which create any type of risks, must be notified (see Art. 33 GDPR).

The controller will be obliged to notify the data subject if this is necessary to protect the data subject (e.g. if financial data of the data subject has been subject and the data subject should take protective measures to avoid further damages) or if the FDPIC requires it after having received the notification (Art. 24 para. 4 nFADP).

Although the controller and the processor must act quickly, the nFADP will not provide for a specific deadline for notification (different from Art. 33 para. 1 GDPR: 72 hours). The wording *"as soon as possible"* provides for a certain degree of discretion. Decisive factors include the extent of the risk and the number of persons affected. The 72-hour period according to Art. 33 para. 1 GDPR may serve as an indicator, which companies should only exceed in particularly serious cases with good reasons. It can be expected that the 72-hour period will factually be observed by many companies in Switzerland, even though not prescribed explicitely.

Finally, it is noteworthy that under Art. 60 et seq. nFADP, non-compliance with the notification obligations will not be sanctioned (unlike under Art. 83 para. 4 let. a GDPR).

Key point:
Data breach notifications

Under nFADP, both the controller and the processor must henceforth report data breaches *"as soon as possible"* (the controller to the FDPIC and the processor to the controller). Although the nFADP does not provide for a fix deadline as under the GDPR, the 72-hour period according to Art. 33 para. 1 GDPR will probably serve as a guideline and could be factually observed by many companies in Switzerland. Under the nFADP, the controller will only have to notify the data subject if this is necessary to protect the data subject or if the FDPIC requires it after having received the notification.

Suggested measures:

— Implementation of internal processes regarding data breach notifications, usually addressed in an internal policy with clear responsibilities to ensure quick internal management of cybersecurity events

3.3. Extended governance rules – (Voluntary) appointment of a Data Protection Advisor

Pursuant to Art. 10 nFADP, companies may appoint a so-called "data protection advisor" (hereinafter referred to as "**Data Protection Advisor**" or "**DPA**"). The DPA is substantially equivalent to the institution initially referred to as the "Data Protection Officer" in the FADP or as today in the GDPR. The requirements for this function, which were previously set out for the DPO, will be incorporated into the nFADP.

The DPA is required to monitor compliance with data protection regulations within a company and advises on data protection issues in a manner independent from the company's management (outside of the line of command). The nFADP goes less far than the GDPR, which provides for an obligation to appoint a data protection officer in certain cases (e.g. if the core activity of the controller or processor consists of carrying out processing operations which, by virtue of their nature, their scope and/or their purposes, require extensive regular and systematic monitoring of data subjects, see Art. 37 GDPR). Under the nFADP, *the appointment of a DPA remains voluntary.* There are no significant benefits in having a DPA appointed aside from the relief of the obligation to notify DPIAs to the FDPIC. The appointment of less formal roles within a company (e.g. a compliance officer taking care of data privacy matters) will also be possible and fulfil the same purposes for internal data privacy management. However, in such cases, the obligation to notify DPIAs to the FDPIC cannot be omitted.

Key point:
Appointment of a DPA

Under the nFADP, companies are not mandatorily required to appoint a DPA, but may appoint him voluntarily. The advantage of an internal DPA consists primarily in the fact that the DPA knows the company (including its structures and employees) and is optimally integrated into the company's communications and interrelationships. Nonetheless, these benefits can also be incurred by a non-formally appointed DPA, such as e.g. a compliance officer or similar employee in charge of data protection matters. The appointment of a DPA only brings the formal advantage that DPIAs need not be conducted.

Suggested measures:

- Implementation of internal processes regarding the appointment of a DPA or (non-formally) an employee in charge of data protection matters;
- Adjustment of hierarchical placements to ensure DPA's independency;
- Training/Certifications of DPA, if required.

3.4. Extended governance rules – Designation of a Swiss representative

According to Art. 14 nFADP, controllers with domicile or residence abroad are henceforth obliged to designate a representative in Switzerland if they process personal data of persons domiciled in Switzerland. This obligation will apply, if (i) data processing is connected to offerings in Switzerland and to monitoring the behaviour of its addressees, if (ii) regular and extensive processing is involved and if (iii) the processing involves a high risk for the personality of the data subjects.

The provision of Art. 14 nFADP more or less "mirrors" the similar provision of Art. 27 GDPR, which provides for an obligation to appoint a representative for controllers or processors without establishment in the European Union under certain conditions. Art. 27 GDPR requires a lower threshold on the level of risks involved, i.e., the obligation to appoint a representative is already triggered with any type of risk whereas in Switzerland only *high risks* will trigger such obligation.

Key point:
Designation of a Swiss representative

Under the nFADP, companies with domicile abroad, which process (i) data in connection with offering goods or services to individuals or entities in Switzerland or monitor their behaviour, (ii) conduct regular and extensive processing and (iii) the processing involves a high risk for data subjects are obliged to designate a Swiss representative. The controller will be obliged to publish the name and address of the representative, for instance in the privacy policy on the website.

Suggested measures:

— Verification whether the obligation to designate a Swiss representative applies and, if yes, appropriate publication of the representative's contact data.

Section 4:
Data processing activities by third parties and cross-border transfers

Under the current Art. 10 a FADP as well as under Art. 9 nFADP, controllers may generally outsource data processing activities by assigning them to a processor either by data processing agreements or by law, provided that (i) the processor only processes in a manner also permitted to the controller, (ii) no statutory or contractual duty of confidentiality forbids such processing and (iii) the controller ensures that adequate data security measures are taken by the processor. As a supplement to the current FADP, a processor may not engage a sub-processor without the prior consent of the controller (Art. 9 nFADP). If the processor is not subject to the nFADP, the controller must ensure that other legal provisions guarantee equivalent data protection and, if necessary, ensure this by contract.

The above being said, it is recommended to undertake written agreements on assigned data processing activities ("**Data Processing Agreements**") and to retain such documentation as evidence. Since there is no general "group privilege" under the nFADP, corporate groups may not regulate their data flows any differently than unaffiliated companies, e.g. through Data Processing Agreements (often referred to as Intra-Group Data Processing Agreements).

Unlike under Art. 28 para. 3 GDPR, the Swiss legislator has refrained from outlining minimum content for Data Processing Agreements. While it is already a widespread practice in Switzerland to sign Data Processing Agreements (Art. 28 GDPR-requirements are meanwhile considered industry-standard), such undertakings will likely increase under the nFADP.

The regime on cross-border data transfers will not substantially change under the nFADP. Pursuant to Art. 16 nFADP, cross-border data transfers will only be permitted on the basis of appropriate safeguards (e.g. if the recipient country provides for an adequate data protection level based on an adequacy decision or, in the case of inadequacy, on the basis of appropriate contractual safeguards). The current FDPIC's state list indicates countries considered to have an adequate data protection level. Although this list is not considered binding, it is considered persuasive by the courts and often followed. Pursuant to Art. 16 nFADP, this list will no longer be maintained by the FDPIC, but henceforth by the Swiss Federal Counsel.

Besides the abovementioned adequacy decision, compliance can also be ensured by means of data transfer agreements (Art. 16 para. 2 lit. d nFADP), in particular in the form of the EU-Standard Contractual Clauses ("**EU-SCCs**"). The FDPIC has publicly stated that the EU-SCCs are the suitable form to conduct data transfer agreements. Finally, compliance can also be attained with the help of binding corporate rules provided that they have been approved in advance by the FDPIC (Art. 16 para. 2 let. e).

According to Art. 61 nFADP, individuals will be liable to a fine of up to 250,000 Swiss Francs if they wilfully disclose personal data abroad in violation of Art. 16 para. 1 and 2 nFADP or assign data processing to a processor without meeting the conditions set forth in Art. 9 para. 1 and para. 2 nFADP.

Caution:

Already in June 2021, with effect as of 27 September 2021, the EU Commission has published an updated version of the EU-SCCs. The FDPIC has recognized these updated EU-SCCs, but has provided a transitional period for agreements concluded before 27 September 2021 (existing contracts) until 31 December 2022 at the latest. As of 1 January 2023, controllers must implement updated EU-SCCs for both existing and, of course, new agreements.

Key point:
Data processing activities by third parties and cross-border transfers

Under the regime of the nFADP, the majority of data processing activities will likely be undertaken via formal Data Processing Agreements, since sub-processing activities are only permitted with the prior consent of the controller. The Swiss legislator has refrained from outlining minimum content of Data Processing Agreements as e.g. under Art. 28 GDPR. Nonetheless, Art. 28 GDPR-requirements have meanwhile become an industry-standard in Switzerland.

The cross-border data flow regime will not substantially change under the nFADP with the exception that the official list of countries providing for an adequate data protection level will henceforth be maintained by the Swiss Federal Counsel (and not by the FDPIC).

The above revision aspects are to be taken seriously as non-compliance will be sanctioned with criminal fines of up to 250,000 Swiss Francs.

Suggested measures:

- Review of data processing activities (esp. implementation and amendments of Data Processing Agreements), as necessary;
- Review of cross-border disclosure of Personal Data (esp. implementation of updated EU-SCCs and data transfer impact assessments), as necessary.

Section 5:
Increased data security obligations (Privacy by Design and Privacy by Default)

The nFADP enshrines the principles of "Privacy by Design" (data protection by technology, Art. 7 para. 1 nFADP) and "Privacy by Default" (data protection by data protection-friendly default settings, Art. 7 para. 3 nFADP) to meet the requirements of the (Schengen-relevant) revised ETS 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and DIRECTIVE (EU) 2016/680 of the European Parliament and of the council of 27 April 2016. Many companies (especially those that have already implemented the GDPR, see Art. 25 para. 1 and para. 2 GDPR) are already familiar with these principles.

Genuinely speaking, the principle of "Privacy by Design" is already known in the basic outlines of the current FADP, duet to the requirement of adequate organizational and technical measures for data security (Art. 7 FADP) and additional data processing principles (Art. 4 FADP, such as e.g. principles of proportionality and purpose limitation which imply to organize processing in a compliant manner already in the design stage). Under the principle of Privacy by Design, companies are required to design their applications in such a way that, among other things, data processing is already designed in advance (by appropriate technical and organisational means) to comply with data protection legislation. The nFADP does not prescribe technology to be deployed but rather suggests a technology-neutral approach. Art. 3 nDPO describes the technical and organisational measures as

— to ensure confidentiality of personal data (i.e. access control, user control),
— to ensure availability and integrity of person data (i.e. data carrier control, memory control, transport control, security and reliability of automated data processing systems),
— to ensure traceability (i.e. data entry control, disclosure control, detection and of data breaches).

Under the principle of "**Privacy by Default**" (data protection-friendly default settings), the controller shall secure with suitable pre-settings that personal data processing is limited to the necessary minimum amount of processing as long as the user does not become active and authorize further processing activities. The Privacy by Default principle can be considered something new under the nFADP (the current FADP does not provide for such rule). According to Art. 7 para. 3 nFADP, the principle of Privacy by Default will only apply *"unless the data subject directs otherwise"*. Therefore, by e.g. means of general terms and conditions, data subjects could waive data protection-friendly settings.

The principles of Privacy by Design is closely tied to the general requirement of data security (enshrined under Art. 8 nFADP). Data security in general must be ensured by various appropriate technical and organisational measures ("**TOMs**"), for example, early pseudonymization or encryption (as possible technical measures), training of personnel and their supervision, restricting access to data on a "need to know" basis or dual control principle etc. (as organisational measures).

Non-compliance with the principles of Privacy by Design or Privacy by Default will not be sanctioned per se. However, if a controller fails to comply with general data security requirements, individuals involved can be held be liable to a fine of up to 250,000 Swiss Francs (Art. 61 lit. c nFADP). Thus, if and to the extent that failure to meet Privacy by Design or Privacy by Default tantamounts to a failure of general data security, then criminal sanctions can be triggered.

Key point:
Privacy by Design and Privacy by Default

By implementing and reviewing data privacy management and technical and organizational measures, companies should ensure compliance with the Privacy by Design and Privacy by Default-principles. It is recommended to review the adequacy of current data security measures (technical and organizational measures), privacy implementation in the design of data processing activities as well as the general default-privacy settings of a company's offerings.

Suggested measures:

— General review of implementation of privacy management within company;
— Review of technical and organizational measures for data security;
— "Frontend"-review of design of the website, business model, terms and conditions and privacy policy;
— "Backend"-review of software development, cookie security and permissions setting.

Conclusion

What can the future bring?

The total revision of the FADP is a significant step for Switzerland to continue maintaining a positive adequacy decision by the EU Commission. The implementation of the main, essential key amendments of the n FADP can be a challenge especially for smaller companies with lower capacities. Nevertheless, we believe that cost-effective measures exist to implement the most relevant features and to prioritize the most important ones. Furthermore, small and medium-sized companies can benefit from exemptions by law or by special governance rules (esp. appointment of a DPA).

Swiss companies that operate already in line with the GDPR resp. have already conducted comprehensive GDPR-upgrade are well prepared and need only to implement limited so-called "Swiss Finishes".

Given the severity of the new sanctions regime imposed under the nFADP, it is recommended to implement the most relevant measures quickly before September 2023.

About CMS Switzerland

Local expertise. Global perspective

CMS Switzerland is a leading full-service law firm in Switzerland with more than 90 lawyers and tax experts and a total staff exceeding 160 employees.

Our history dates back to more than 80 years, and our reputation in the market for legal and tax services has been strong and established ever since. We serve our clients from our offices in Switzerland's main business centers, Zurich and Geneva.

As part of the global CMS organisation, CMS von Erlach Partners is one of few international law firms in Switzerland that can offer you both domestic and international advice. As your business partner, we offer you our local expertise combined with the global reach and capabilities of CMS international, with access to 5,000+ lawyers worldwide in 75+ offices in more than 40 countries. We are able to put quickly in place diverse, agile, cross-border teams of experts from all disciplines to serve your needs. No matter the size of your company, which jurisdiction you are based in or the legal challenges and issues you face – you always have our full attention. Our clients profit from our in-depth sector knowledge, our global reach and our ability to anticipate challenges.

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Cúcuta, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

---

cms.law