2 DECEMBER 2020

Revised Federal Act on Data protection

On September 25, 2020, after more than two years of parliamentary negotiations, the Swiss parliament passed the revised Federal Act on Data Protection (FADP). Despite a total revision of the law, the basic principles of data processing (in particular transparency, purpose limitation, proportionality and data security) remain unchanged and apply as before. As under applicable law, data processing continues to be considered lawful if it occurs in compliance with these data processing principles and no personality rights are violated. This means that only in certain situations justification by consent, legal basis or overriding private or public interests is necessary. Despite the alignment with the EU General Data Protection Regulation (GDPR) in many points, Switzerland still deviates from the GDPR in this respect.

Nevertheless, there are various new regulations under the revised FADP and various points are adapted to the GDPR: data of legal entities are no longer protected, information obligations of the controller have been extended and numerous data protection governance obligations have been introduced (e.g. records of processing activities, data protection impact assessment, obligation to report a data breach, optional data protection advisor, etc.). The revised FADP also contains a more stringent catalog of penalties and enhances the competences of the Federal Data Protection and Information Commissioner (FDPIC). In case of a violation of the regulations of the revised FADP, the responsible person in a company can be personally liable for fines of up to a maximum of CHF 250,000. For this reason, the NKF data protection team has drafted this compliance checklist. It is intended to help you assess the need for action with regard to the implementation of new data protection regulations in your company. The revised

FADP is not expected to come into force before 2022, but it does generally not provide for a transitional period (with a few exceptions). Therefore, companies must have taken the necessary measures by the time the revised law comes into force. If you have any questions, please do not hesitate to contact the authors listed below.

Subject	Article in revised FADP	Criteria	What is new?
Scope *Is your company affected?*	Art. 2, 3	☐ Processing of personal data in Switzerland ☐ Processing of personal data outside of Switzerland, but with effect in Switzerland	Territorial scope: Data processing „effects" in Switzerland trigger the applicability of the revised FADP.
Data *What kind of data is affected?*	Art. 5	☐ Personal data (all information relating to an identified or identifiable natural person) ☐ Sensitive personal data (data on religious, ideological, political, trade union-related views or activities; health; intimate sphere; racial or ethnic origin; genetic data; biometric data; data on administrative or criminal proceedings and sanctions; data on social security measures)	Data of legal entities are no longer protected under the revised FADP. Genetic data and biometric data (that unequivocally identify a natural person) are now explicitly included in the definition of sensitive personal data. The previous obligation to register data files is no longer applicable.
Profiling *Do you conduct profiling?*	Art. 5, 6	☐ Profiling: automated processing of personal data consisting of using such data to assess certain personal aspects relating to a natural person ☐ High risk profiling: profiling which involves a high risk to the personality or fundamental rights of the data subject	Profiling is comparable to the processing of a „personality profile" under the current law. Profiling with a high risk is subject to the same qualified data processing requirements that apply to sensitive personal data. This means in particular that consent must be given explicitly if the data subject's consent to processing is required.
Data security *Is your data secure?*	Art. 7, 8	The controller and processor must ensure data security by means of adequate technical and organizational measures: ☐ Appropriate technical and organizational measures (so-called TOMs) ☐ Implementation of privacy by design and privacy by default principles	Technical and organizational measures for data security must now be taken into account when planning to process data (privacy by design) and when programming/drafting the basic settings (privacy by default).

Subject	Article in revised FADP	Criteria	What is new?
Data processing *Is data processed by a processor?*	Art. 9	☐ Processing of personal data assigned to a processor remains lawful (unless a statutory or contractual duty to secrecy prohibits the assignment) ☐ A data processing agreement must be concluded in order to ensure that data is only processed by the processor in a manner as permitted for the controller itself	No changes: As under the current law (art. 10a), processing may be assigned to a processor if the controller ensures that the processor is able to guarantee data security and that data is processed only in a manner as permitted for the controller itself.
Responsibility *Who is responsible for data protection compliance within a company?*	Art. 10	As the board of directors exercises overall control over the company, the board of directors is ultimately responsible for compliance with the applicable data protection laws. However, the board may delegate this responsibility to the executive management or to an internal or external data protection advisor (who must be able to act independently of the executive management): ☐ Has the company appointed a data protection advisor? ☐ Has a person within management been designated to ensure the FADP compliance? ☐ Has a person in each respective local entity/business entity been determined to ensure FADP compliance? ☐ Is the independence of the data protection advisor guaranteed and are her/his obligations clearly defined?	The responsibility for compliance remains with the controller. The internal data protection officer („DPO") is now referred to as „data protection advisor". Companies may appoint (but must not) a data protection advisor, who is the contact point for the data subjects and for the competent data protection authorities responsible for data protection matters in Switzerland.
Record of processing activities *Do you have to keep a record of the processing activities?*	Art. 12	☐ List of all processing activities, including the purpose of processing, the categories of data, a description of the measures taken to ensure data security, the indication of the countries for international data transfer and the corresponding guarantees, etc. ☐ Data retention schedule, which lists the retention period of each data category	New obligation for the controller and processor. The Federal Council may provide for exceptions for companies with less than 250 employees if their data processing involves a low risk of privacy breaches.

Subject	Article in revised FADP	Criteria	What is new?
Representative *Who needs to appoint a representative?*	Art. 14	Controllers with domicile/residence outside of Switzerland designate a representative in Switzerland if they process personal data of data subjects in Switzerland and the data processing fulfils the following conditions (cumulative): ☐ The data processing is connected to the offering of goods or services in Switzerland ☐ The data processing is connected with the monitoring of the behavior of persons in Switzerland ☐ The data processing is comprehensive and regular and involves a high risk to the personality of the data subjects	This is a new obligation for a controller with domicile/residence outside of Switzerland.
Data transfer *What must be considered when personal data is disclosed abroad?*	Art. 16	Legal basis for transferring data abroad: ☐ It is recognized by the Federal Council that an equivalent level of data protection exists in the country concerned, otherwise ☐ Group-internal data transfer agreements/data protection regulations (so-called binding corporate rules) ☐ Recognized standard contractual clauses of the EU or a FDPIC model contract	No changes to the basic principles for data transfers. From now on, the Federal Council can issues adequacy decisions on other country's level of data protection (the country list of the FDPIC is no longer applicable). The obligation to notify the FDPIC when approved standard contract clauses are used no longer applies. Note: In light of the ECJ's Schrems II decision, the Privacy Shield is no longer a sufficient legal basis for data transfers to the US (→ implement other privacy measures). According to the FDPIC, it must be checked for each third country whether the local public law respects the contractual regulations used (e.g. standard contract clauses).
Duty to inform *What measures need to be taken?*	Art. 19	☐ Privacy policy in place that provides data subjects with all required information in order to assert their rights under the FADP. The following minimum information must be provided: (i) the identity and contact details of the controller, (ii) the purpose of the processing, (iii) where applicable, the recipients to whom the personal data is disclosed, (iv) if the data is disclosed abroad, the State and, where applicable, the guarantees (e.g. binding corporate rules), (v) where applicable, the categories of personal data processed ☐ Cookie policy (incl. consent requirement for non-technical cookies)	Compared to the applicable law, there are concrete and extended information obligations with regard to the processing of all kind of personal data, not only to the processing of sensitive personal data or of personality profiles.

Subject	Article in revised FADP	Criteria	What is new?
Data processing impact assessment (DPIA) *When do you have to perform a DPIA?*	Art. 22	If intended processing may lead to a high risk to the data subject's personality or fundamental rights, a DPIA must be conducted: ☐ Is there a documentation for the execution of a DPIA (incl. methodology)? ☐ Is there a register of performed DPIA?	New obligation for the controller. A „high risk" is particularly given if new technologies are used or if sensitive personal data are processed on a regular and extensive basis. The DPIA must contain a description of the planned processing, an assessment of the risks to the personality or fundamental rights of the data subject and the measures to protect personality and fundamental rights.
Data breaches *Do you have a notification obligation?*	Art. 24	Procedures in place to notify the FDPIC as soon as possible in case of a data security breach: ☐ Data breach response and notification plan (incl. notification form) for possible future cases of data security breaches ☐ Is there a register in which data security violations are documented?	New notification obligation of the controller if the violation of data security is likely to lead to a high risk to the personality or fundamental rights of the data subject. Data subjects must be informed if it is necessary for their protection or if the FDPIC requests it.
Data subject rights *Which rights must be taken into account?*	Art. 25, 32	Are internal procedures in place to answer the following requests from data subjects: ☐ Information rights ☐ Right to rectification ☐ Right to erasure ☐ Automated decision-making	The rights of the data subjects are slightly extended or specified under the revised FADP. This applies in particular to the rights of data subjects in connection with automated decisions-making.
Right to data portability *Do you have to hand out data to a data subject?*	Art. 28	☐ Upon request, a controller must be able to hand out to data subjects their personal data in a standard electronic format (if the data controller processes the data by automated means and 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)	New obligation for the controller. In principle, the data must be provided free of charge, but the Federal Council may provide for exceptions, in particular if the effort is disproportionate.
New competences of the FDPIC/ sanctions *Which are the measures and sanctions a company is facing in case of a FADP violation?*	Art. 51 et seq.	Under the revised FADP, the FDPIC may investigate (ex officio or upon notification) data processing activities and may, if regulations are violated, impose administrative measures (e.g. stop the processing). In case of breach of certain obligations under the FADP, **individuals** may face fines of up to CHF 250'000. ☐ Check the scope of your D&O insurance ☐ Specific data protection insurance (conclude an insurance or check the scope of an existing one)	Check insurance coverage for fines for data protection and security breaches.

This compliance checklist is only intended to provide you with a brief overview of the most important new FADP regulations as far as known today (as of November 2020). It is not designed to provide legal advice.

If you have further questions or comments on this topic, please reach out to your regular NKF contact.

Authors /Contact

Clara-Ann Gordon
Partner, Technology/Data Protection
clara-ann.gordon@nkf.ch

Dr. András Gurovits
Partner, Technology/Data Protection
andras.gurovits@nkf.ch

Janine Reudt-Demont
Counsel, LIfe Sciences/Healthcare
janine.reudt-demont@nkf.ch

Eric Neuenschwander
Associate, Technology/Data Protection
eric.neuenschwander@nkf.ch

NIEDERER KRAFT FREY

NKF Technology Team

Dr. András Gurovits
Partner
IT, Telecoms, Outsourcing

Clara-Ann Gordon
Partner
Cloud, Outsourcing

Janine Reudt-Demont
Counsel
Life Sciences, Healthcare

Anne Huber
Associate
Smarthome, Smartgrid

Binderiya Gan-Ayush
Associate
Cyber Incidents, Cloud

Eric Neuenschwander
Associate
Data Protection, FinTech

Luisa Egli
Junior Associate
AI, Blockchain

Thomas van Gammeren
Junior Associate
FinTech, Robo-Advisory