walderwyss

Walder Wyss Ltd.
Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

Telephone +41 58 658 58 58
Fax +41 58 658 59 59
www.walderwyss.com

David Vasella
Partner
Dr. iur., CIPP/E, CIPM, FIP
Attorney at Law
Direct +41 58 658 52 87
david.vasella@walderwyss.com

Revised Swiss Data Protection Legislation: Implementation for SMEs

9 March 2023

This document contains a checklist for implementing the revised Swiss Data Protection Act (**nFDPA**) and the related revised Data Protection Ordinance (**nFDPO**). Both will enter into force on 1 September 2023. There are no transition periods except for some obligations.

The checklist is designed for smaller private entities (not for public bodies). Larger organizations will require various internal procedures in order to comply with the requirements under the nFDPA and nFDPO, even if these do not expressly require it.

Mandatory tasks are highlighted in red, tasks that may be mandatory in yellow and tasks that may be sensible but are optional in green.

This checklist only considers the nFDPA and the nFDPO and to some extent confidentiality obligations, but neither requirements under sectoral regulation nor the European General Data Protection Regulation (**GDPR**). The GDPR must be complied with – in addition to the nFDPA – if a Swiss company has an establishment in an EEA county, intentionally makes offers to individuals in the EEA or monitors the behavior of individuals in an EEA county (e.g. through some form of online tracking), and where internal or external requirements demand compliance with the GDPR.

The checklist is not exhaustive and is not legal advice.

1. Policies and Documentation

Unlike the GDPR, Swiss data protection law does not recognize any general documentation obligation and accordingly no obligation to issue guidelines. However, it is *de facto* mandatory to set out at least the essential principles, in the form of a directive or instructions.

Minimum requirements:

— Thinking through the organization and its processes

— Setting out essential instructions and tasks as a guideline or at least a two-pager for employees

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
PN	A document with general instructions for dealing with personal data	No, but useful as a basis for proper correct internal delegation of responsibilities, as instructions under the employment agreement, and as a basis for training.	n/a
Other policies and guidelines	Documents with additional instructions, for example for the proper use of IT resources and for some forms of monitoring by the employer.	Not directly, but often useful, and investigating e-mail and other electronic data requires appropriate prior information, according to the Swiss Federal Data Protection and Information Commissioner (FDPIC).	Article 6 and 19 nFDPA; article 321b Code of Obligations
"Two-pager" on data protection	A short document for employees with actionable information and advice on dealing with data protection matters, e.g. when new tools are to be used on a website, when processing is new or changed, in case data subject requests or security breaches, and on keeping personal data confidential.	Not expressly but usually mandatory if there are no other policies and processes exist. It can also be used as an overview and field guide in larger companies.	n/a
"Logbook" on data protection	A document (or an intranet page etc.) where data protection matters can be logged (e.g. data subject	No, the nFDPA does not require systematically recording such matters. However, it can be helpful internally, and if	n/a

	requests, security breaches, data protection impact assessments carried out etc.)	necessary also externally, e.g. in the event of the sale of a company.	
Training	Data protection training is useful, especially for employees who have specific tasks in the context of data protection compliance (e.g. in HR, IT, legal, etc.).	No, data protection training is not mandatory but in fact will usually be required, in a form suitable for the company.	n/a

2. Data Protection Organization

The nFDPA has only few express requirements for the organization in the area of data protection. In fact, however, most companies will have to take certain organizational measures.

Minimum requirements:

— Thinking through the needs, existing resources and processes and responsibilities of the company

— If necessary, appointing the required functions and define their role in a policy or instruction

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
Appointment of a Data Protection Advisor (DPO)	A DPO is responsible for proactively and reactively monitoring compliance with data protection within the company and as a contact point both internally as well as for data subjects and for the FDPIC.	No, the appointment of a DPO is not mandatory under the nFDPA, even in the case of high-risk processing. However, it is perceived as part of compliance and may be expected by business partners.	Article 10 nFDPA; articles 23 and 25 et seq. nFDPO
Appointing additional data protection functions	Compliance with data protection cannot be managed with external resources alone – certain internal resources are almost always necessary, at least dedicated subject-matter experts or contact persons. In addition, the management or the board should understand the topic sufficiently and, above all, take it seriously.	Not directly, but if the board ignores the issue there may be personal liability risks. An internal body should therefore be responsible with data protection. For larger companies, contact persons should be designated in the business units as well as support functions.	n/a
Swiss Representative	In exceptional cases, the nFDPA requires foreign companies to appoint a representative in Switzerland.	Yes, if, exceptionally, the relevant conditions are met.	Articles 14 et seq. nFDPA

3. Records of Processing Activities and Processing Regulations

Companies are under an obligation to keep an inventory of its processing, the "records of processing activities" (or "ROPA"), except for SMEs which may be exempt from this obligation.

Minimum requirements:

— Completing records of processing activities and keep it up to date (unless the SME exception applies)

— Deciding if processing regulations must be kept; if yes, creating these regulations

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
Records of processing activities (ROPAs)	A list of the data processing activities with certain minimum information (e.g. in the form of an Excel document or via the Walder Wyss platform).*	Yes, except for SMEs with less than 250 employees as of 1 January, provided that no "sensitive personal data" is processed on a large scale and no "high-risk profiling" takes place.	Article12 nFDPA; Article23 nFDPO
Process for updating ROPAs	It makes sense to define a process for keeping the ROPAs up-to-date, e.g. as instructions to the business to see if new or changed processing activities require an update, if yes, inform the data protection expert.	No, such a process is not mandatory. However, the ROPAs must be kept up-to-date. At least a very basic process will be required.	Article 12 para. 1 nFDPA
Processing regulations	A data protection manual for one or several processing operations that describes the data protection organization, how the systems work, the steps	Yes, but only for automated large-scale processing of sensitive personal data and for high-risk profiling.	Articles 5 et seq. nFDPO

* We provide a platform for data protection projects including a tool for collecting and keeping ROPAs.

	of processing and the security measures. The regulations can refer to existing documents and do not have to be detailed.		

4. Information and Privacy Notices

Under the nFDPA controllers must inform the data subjects how they collect and use personal data and provide certain minimum information about their processing. Unlike under the current FDPA, this applies not only for sensitive data or unexpected processing. An intentional breach of the information obligation may be liable to a fine.

Minimum requirements:

— Drafting and posting of a general privacy notice (PN)

— Drafting and sharing an HR PN with employees

— Reviewing contracts, GTC and other documentation, and if necessary adding references to the PN or removing outdated information about data protection (see Section 6 – Contractual Provisions)

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
General PN	A general privacy notice (PN) posted on the company website, which explains the processing of (end) customer data, data of contact persons of suppliers and B2B customers and other persons, in particular the collection of data from third-party sources.	Yes, a PN is mandatory, and a general PN on the website is often a *de facto* mandatory measure.	Articles 19 et seq. and Article 61 nFDPA; article 13 nFDPO
Online PN	A PN that explains cookies and other technologies but also other processing in an online scenario (in apps, in a contact form, through electronic newsletters, etc.).	Yes, such a PN is mandatory if personal data is processed online. It also meets current expectations of the public in Switzerland.	Article 45c of the Telecommunications Act
References to PNs	PNs should be referred to in the appropriate places (e.g. in terms and conditions, in online forms and in online shops, in invoices, in correspondence etc.).	The requirements for references to PNs are not yet clear, but where possible, the data subjects should be made aware of the relevant PN at the relevant touchpoints.	Articles 19 et seq. nFDPA; Article13 nFDPO

5. Data Subject Rights

As under the FADP, data subjects have certain rights under the nFDPA (access right, rectification right, right to object, portability right, right to be heard in case of automated individual decision-making).

Minimum requirements:

— Thinking through procedures for requests for data subjects

— If necessary, defining the process in a policy

— Ensuring that data can be retrieved, updated, extracted, and deleted

— Checking if relevant decisions are made automatically (usually not)

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
A Process description for dealing with subject rights	Subject right requests must usually be answered with a period of 30 days.	A separate process for dealing with subject rights makes sense, but is de-facto mandatory only for complex organizations or for frequent requests. For smaller organizations, a guideline or general instruction will be sufficient – they can obtain legal advice in individual cases.	Article25 et seq. nFDPA; articles 16 et seq. nFDPO
Template correspondence	Standard texts and answers to subject requests (references to subject rights e.g. when automated individual decisions are communicated, acknowledging receipt of subject requests, request for identification, rejection of requests etc.) are useful in case of frequent requests or in order to standardize responses in a decentralized data protection organization.	No, except for very complex organizations or very frequent requests for data subjects.	n/a
Special requirements: Data portability	Under the nFDPA, data subjects have the right to obtain certain data in a machine-readable form or	The portability right applies to data obtained from the data subject and for behavior (transaction, use…) data.	Article21 nFDPA

	to have it transmitted to another controller ("data portability").	Where applicable, the company must be able to retrieve the data in a common format in a timely manner.	
Special requirements: Automated individual decision-making	"Automated individual decisions" are decisions that are taken automatically and have significant effects on data subjects (e.g. automatic refusal or termination of a contract). Special rights apply for the data subjects in these cases.	In case of automated individual decisions, the data subject must be informed in advance in a PN or in each individual case that the decision was automated and that the data subject has certain rights.	Article21 nFDPA

6. Contractual Provisions

In certain constellations, the nFDPA has obligation to conclude a certain form of contracts, especially in the case of processing on behalf of a controller. It may be a criminal offence to involve a processor without an appropriate data processing agreement.

See sec. 4 – Information and Privacy Notices and sec. 7 – Transfers Abroad

Minimum requirements:

— Reviewing where processors are used

— Reviewing the existing agreements with processors

— Entering into a data processing agreement if necessary

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
Data processing agreement (DPA)	As a rule, a template DPA will be required. DPAs must be concluded with existing processors, unless such agreements have already been agreed.	Yes. Using a processor without a sufficient DPA can be liable to a fine.	Article 9 nFDPA, article 7 nFDPO
Agreement between joint controllers	Several controllers may be joint controllers if they work together in some form of a division of labor. An agreement can clarify responsibilities for data protection.	No, not under Swiss law, but such an agreement is often a sensible measure. It also makes it easier to respond to subject requests.	n/a
Standard clauses in GTC and other agreements	Reference to the relevant privacy notice (PN; usually the general PN on the website) in terms and conditions and in other agreements (application forms, etc.). Potentially use standard wording in purchasing or delivery conditions and other agreements.	No, not under Swiss law, but such references are a de-facto requirement at least in agreemens with end customers.	n/a

Confidentiality agreements with third parties	Standard confidentiality clauses or agreements ("NDAs") with third parties who receive personal data and/or secret data.	Yes, if personal data and especially if secret data is shared with third parties (i.e., not processors), confidentiality and purpose limitation is to be ensured by the third party.	Article 6-8 and 62 nFDPA; article 321 Criminal Code, etc.

7. Transfers Abroad

Like the current FADP, the nFADP restricts the transfer of personal data abroad if the recipient country does not provide an adequate level of data protection. These countries are listed in an annex to the nFDPO. If no exception applies, a specific type of agreement must be concluded with the recipient for such disclosure. In case of disclosures abroad data processing agreenments or other agreements may also be required (see Section 6 – Contractual Provisions).

Minimum requirements:

— Reviewing if data is shared with a recipient abroad

— Reviewing whether the relevant countries are outside the EEA; reviewing applicable agreements and, if necessary, entering into the standard contractual clauses with adjustments for Switzerland

— in this case, carrying out a "Transfer Impact Assessment"

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
EU Standard Contractual Clauses	A special type of agreement ("SCC") recognized by the EU and Switzerland that may permit transfers to countries without adequate protection (e.g. the USA, India or China; "third countries". The SCCs must be adapted selectively to Swiss law.	Yes, unless an exception or other basis for the transfer applies. The transfer of personal data to such countries without sufficient safeguards may be punishable.	Articles 16 et seq. and Article 61 nFDPA; articles 9 et seq. nFDPO
Updating existing contracts	If agreements with recipients in a third country do not use the SCCs or use the old version of the SCCs, these agreements must be updated as soon as possible.	Yes, where such a contract exists. This should be reviewed.	Articles 16 et seq. and Article 61 nFDPA; articles 9 et seq. nFDPO
«Transfer Impact Assessment»	The SCCs only apply to the recipient, but not to local authorities, who may be able to access data on the basis of local law. In order to assess the risk of lawful access that may be unacceptable from a Swiss	Yes. The SCCs are only sufficient if a transfer impact assessment has shown that the residual risk of unacceptable access to authorities is sufficiently low. This is especially true when secret data is transmitted abroad.	Articles 16 et seq. and Article61 nFDPA; articles 9 et seq. nFDPO

	point of view, this risk must be assessed, usually by means of a “transfer impact assessment”.		

8. Compliance and Risk Assessments

Swiss law does not expressly require processing to be reviewed proactively, but if the processing principles are not complied with, this is a breach of data protection law. In addition, in case of processing that is likely to carry high risk, risks for data subjects are to be assessed through a "data protection impact assessment".

Minimum requirements:

- Considering if the processing activities comply with the principles, in particular if as little data as possible is kept, about as few people as possible, and not longer than necessary, and if data is made accessible to as few people as possible and is only used as originally communicated or expected
- Taking corrective action as appropriate
- Considering if the a data protection impact assessment ("DPIA") is to be carried out
- If necessary, carrying out a DPIA

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
Reviewing all processing for conformity and risks	A general review of all processing activities for compliance with data protection requirements (especially the processing principles) and for high risks	No, Swiss law does not expressly require such a review (but of course data protection must be complied with).	n/a
Data Protection Impact Assessment ("DPIA")	A structured assessment of the risks of a particular processing activity for data subjects, usually on the basis of a template DPIA.	Yes, if processing is likely to entail high risk for data subjects, especially if sensitive personal data (e.g. health data) are processed large-scale, if extensive public areas are monitored systematically, and in the case of high-risk profiling. The DPIA must be kept for at least two years after the data processing activity ends.	Article 22 nFDPA; Article 14 nFDPO

9. Employee Data

Personal data about individuals in a somewhat weaker position dependency are processed to a greater extent in the employment context. There are also additional legal risks for companies due to potential claims brought by employees. Data protection in an HR context is therefore particularly important, even for companies that otherwise process personal data only in the B2B sector.

Minimum requirements:

— Drafting and sharing a privacy notice (PN) with employees

— Drafting a PN for job applicants

— Considering if the processing principles will be complied with for employee data (see sec. 8 – Compliance and Risk Assessments)

— See also sec. 11 – Data Deletion.

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
PN – employees	A privacy notice (PN) for employees explains how employee data is processed, from the time they are hired.	Yes, a PN for employees is mandatory. It should be referenced in the employment agreement or staff regulations.	Article 19 et seq. and article61 nFDPA; article 13 nFDPO
PN – applicants	A PN for job applicants explains how applicant data is processed, up until the hiring or deletion in case an application is rejected.	Yes, unless processing applicant data is included in the PN for employees, which is often not the case. Information about data processing in a standard response to applications may also make sense.	Article 19 et seq. and Article61 nFDPA; article 13 nFDPO
Non-disclosure undertakings with employees	An express confidentiality provision in the employment agreement, in staff regulations or in a separate document.	No, but especially useful if the company has non-disclosure agreements with third parties or processes data that is subject to professional secrecy obligations.	n/a (article 321a para. 4 CO; article 321 Criminal Code, etc.)

10. Data Security

The nFDPA and the nFDPO set a framework for the minimum security of personal data. It is unclear of a breach of any of these measures is liable to fines. There is therefore a risk of criminal liability if adequate security is not ensured. Where sensitive data is processed, there may also be an obligation to keep a log of various processing activities, including read-only access to such data.

Minimum requirements:

— Reviewing if IT systems or components are sufficiently secure or seeing with IT which security standards and processes exist and if these are up to date

— Reviewing if the requirements for a logging obligation are met

— Thinking through how security breaches are dealt with, defining a process, if necessary, and walking the relevant persons or functions through the process

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
Ensuring data security	The nFDPA requires that personal data be adequately protected against loss, damage and access. For this purpose, appropriate technical and/or organizational measures must be taken (e.g. protection of IT systems and physical infrastructure, ensuring the need-to-know principle when IT is configured and administered, preventing access and changes to data at rest, protection data in transit, ensuring data can be recovered, updating systems and applications, ensuring access and changes can be traced, ensuring data breaches are handled properly). These reviews and conclusions should be documented.	Yes. Not providing for an appropriate level of data security may be liable to a fine (disputed).	Article 8 nFDPA; articles 1 et seq. nFDPO

Keeping logs	In certain cases, controllers and processors must log operations such as saving, changing, reading (!), transferring and deleting data, as well as who has carried out which processing at which time, and if necessary to whom data is disclosed. Logs must be kept separately from the production environment for at least one year.	Yes, if sensitive personal data is processed automatically on a large scale or if high-risk profiling takes place, provided that other measures do not ensure data protection.	Article 4 nFDPO
Process for dealing with security breaches	If there is a data breach (if data is lost, deleted, destroyed, changed or disclosed accidentally or as a result of an external or internal attack), the breach must be reported (i) to the FDPIC where it is likely to result in high risks for the data subjects, and (ii) to the subjects where this is necessary for their protection. In addition, the breach, its effects and the measures taken must be documented. The documentation must be kept for two years from the date of notification of the breach. Processors must notify the controller of any data breach.	Usually yes, because security breaches are common, and a violation of the reporting obligation is a breach of data protection law, even if it is not liable to a fine.	Articles 22 and 24 para. 3 nFDPA; article 15 nFDPO

11. Data Deletion

Personal data may only be kept for as long as it is necessary for processing or for compliance with statutory retention obligations. If they are not subsequently deleted or anonymized, this constitutes a violation and generally increases risks for the company as well as the data subjects. Ensuring deletion is a difficult and usually time-consuming task.

Minimum requirements:

— Considering if data will be deleted and if applicable retention periods are known

— If necessary, setting retention periods

— Installing a deletion process or, if necessary, deleting data manually on a regular basis

Document/Task	*Notes*	*Mandatory?*	*Legal Basis*
Ensuring timely data deletion	In principle, personal data may only be kept for as long as is necessary for the processing purposes or for compliance with retention obligations. Once these periods expired, the data must be deleted or anonymized.	Yes. Storage for too long is a breach of data protection law, increases risks when security breaches occur, and makes it more difficult to deal with data subject rights.	Article 6 para. 2-4 nFDPA
Setting retention and deletion periods	For regular data deletion, retention periods must be defined for each data category. Different retention obligations may apply.	Yes. If data is deleted too late there is a breach of data protection (cf. above), and deleting it too early can violate retention obligations.	Various regulations in the field of HR, tax, commercial law, etc.
Defined deletion processes (comprehensive or application-specific)	A rule-compliant deletion requires not only the determination of the retention periods, but also erasable systems and a corresponding system configuration.	In fact, mostly yes, a manual deletion is illusory.	Article 6 para. 2-4 nFDPA