Monthly
Newsletter
October 2022

Data

Implementation of the New Data Protection Act: Step 1 - Preparation

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

1.
The new data protection law will come into force on 1 September 2023, with no transition period. The new requirements must be met from day one.

2.
The necessary implementation measures should be addressed early on. They can be prioritized on a risk-based and resource-oriented basis and bundled into three implementation steps.

3.
Step 1 includes preparation, fact-finding and certain preliminary decisions. In step 2, external measures are implemented. Step 3 focuses on the implementation of internal measures.

1 Overview

On 31 August 2022, the Federal Council decided that the completely revised Swiss Data Protection Act (**nDPA**) will enter into force **on 1 September 2023**, including the new implementing Data Protection Ordinance (nDPO). There will be no transition period. Fortunately, there is an implementation period available of about a year until the entry into force.

This time should be used wisely and the implementation of the new requirements should be initiated early on, with project completion scheduled by August 2023 at the latest. The **effort required for the implementation** should not be underestimated and will depend on the individual situation.

2 What Changes - and What Stays the Same?

The **basic principles of Swiss data protection law** remain the same. Data processing requires (unlike under the EU General Data Protection Regulation (**GDPR**)) neither consent nor special justification, as long as the general processing principles are adhered to, the data subject has not expressly objected to the data processing and sensitive personal data is not disclosed to third parties. The **general processing principles** (namely lawfulness, transparency, purpose limitation, proportionality, data accuracy and data security) also remain largely the same in terms of content.

Changes result, however, from the **increased level of detail** of the legal regulation, the extensive **formal requirements** and the newly introduced **sanctions regime**. In addition, the definition of personal data will be restricted, i.e. the nDPA will only refer to data of **natural persons** (individuals) - legal entities will no longer fall within its scope of protection.

3 Relevance of Timely Implementation

The requirements of the nDPA must be met from 1 September 2023. From then on, the new **sanctions regime** providing for specific fines will be applicable. In terms of amounts, these fines (of up to CHF 250,000) are not comparable to those under the GDPR (of up to 4% of global turnover or EUR 20 million, whichever is higher). The big difference, however, is that under the nDPA, fines are not targeted at the company, but at the responsible person. This can be the formal decision-takers (e.g. management, officers, board of directors) or employees with independent decision-making authority in their area of activity (e.g. division or department heads, centralized functions, etc.).

4 Implementation in Three Steps

Against this background, a risk-based and resource-oriented **prioritization** of implementation measures is recommended. How much **effort for the implementation** is to be expected depends on how much attention was given to the topic of data protection in the past. If, for example, the GDPR has already been implemented (e.g. due to internal group requirements), only few additions to the existing measures will be necessary. If only (or not even) the minimum requirements of the current DPA have been implemented so far, more effort will have to be expected.

In the following, we present a three-step **implementation plan** (**roadmap**) and elaborate on the first step in more detail. Steps 2 and 3 will be addressed in two follow-up newsletters. This roadmap can serve as a guide for implementation - but will have to be adapted to the specific situation and individual starting point in each case, and may have to be supplemented with industry- and sector-specific requirements.

5 Timeline

5.1 Until the End of 2022

Without being connected to the implementation of the requirements of the nDPA, the Federal Data Protection and Information Commissioner (**FDPIC**) requires that **standard contractual clauses (SCC) concluded before 27 September 2021** must already be replaced before the end of this year. Further details on this can be found in our newsletter of May 2022.

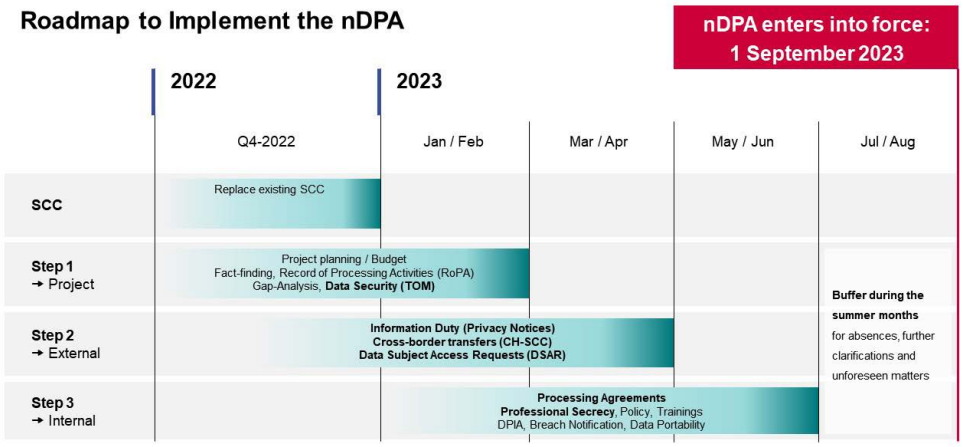
In a separate workstream, the relevant cross-border data transfers should thus already be identified and addressed with SCC adapted to Swiss law **until the end of 2022**. Ideally, this can be combined with step 1 below for the implementation of the nDPA, in particular the fact-finding aspect.

The nDPA introduces new obligations and risks of fines.

5.2 Roadmap for the Implementation of the nDPA

The timeline for implementation depends to a high degree on how data protection has been addressed in the past, and on the scope and complexity of the data processing undertaken. In any case, completion of the implementation project should be targeted before or by mid-August 2023. Any absences or restricted information flows during the summer months of July/August must also be taken into account. Ideally, this time should be reserved as a buffer. Thus, the following schedule can serve as guidance:

- **Q4-2022 to January/February 2023 - Step 1**: Certain preliminary decisions need to be taken, project coordination (including budget) needs to be addressed, and a fact-finding exercise (including the data security measures) can serve as basis for a gap analysis.
- **From November/December 2022 to March/April 2023 - Step 2**: Focus on the implementation of measures with an external effect (whereby the focus here will depend largely



on the respective business sector as well as on internal requirements of the company or group).

– **From 2023 to May/June 2023 - Step 3**: Focus on the implementation of internal measures (prioritizing the areas which are subject to sanctions).

It is advisable to identify at an early stage those areas in which a greater effort is to be expected due to the specific situation (e.g. if extensive fact-finding efforts are to be expected or if it becomes apparent that a large number of contracts must be adapted). If necessary, such measures can then already be addressed in prior steps.

6 Step 1: Preparation

6.1 GDPR Assessment

At an early stage, it should be addressed whether the **requirements of the GDPR** must be observed due to the business model or the data processing carried out (Art. 3 (2) GDPR). If so, this must be taken into account when implementing the nDPA. If not, the question arises as to whether the GDPR requirements should not be implemented nevertheless (e.g. for reputational reasons or if there are within an international group already GDPR-compliant processes and documentation on which to build on).

If there are already GDPR-compliant processes and corresponding documents, these are a good starting point for implementing the nDPA. Since there are still certain differences between the nDPA and the GDPR, certain "**Swiss Add-Ons**" must be implemented in addition to the existing GDPR measures. This concerns in particular the areas of cross-border transfers, privacy notices and data subject access requests. Further details on this can be found in our newsletter of December 2021.

6.2 Project Coordination

To **prepare for the implementation**, a suitable project coordination should be set up early on and the necessary resources and contact persons should be identified and involved. This includes in particular the relevant know-how bearers from data protection-relevant areas (such as marketing, IT, HR, etc.), whose detailed knowledge of the company's internal processes and data processing is indispensable for the implementation.

6.3 Fact-Finding

In a fact-finding exercise, the information required for the implementation will need to be collected. The aim should be to identify the current **data collection**, the **data processing** carried out and any **cross-border data transfers**. As a basis for the next steps, it should be documented in an easily accessible manner how personal data is collected, who uses or otherwise processes it and for what purpose, whether this is done with the help of external service providers, whether personal data is transferred abroad or accessed from there (and if so, which countries are involved), where the personal data is stored, etc.

Generally available templates, existing documents (e.g. internal group registries) and checklists regarding the relevant points can be helpful for the fact-finding. If the information is not already available, it can be obtained through interviews with the relevant contact persons.

6.4 Processing Register

For the central collection and consolidation of information, a **processing register** (or **record of processing activities (ROPA)**) should already be created at this point (Art. 12 nDPA). There is an **exception** to the requirement to keep a processing register for companies with fewer than 250 employees, provided no high-risk processing is carried out (Art. 24 nDPO). However, even companies that fall under this exemption must deal with their processing activities in detail and implement the other requirements of the nDPA. In most cases, it is therefore advisable to keep a processing register even if there is no legal obligation to do so.

6.5 Data Security

As assessments (and potential adjustments) in the area of **data security** are usually time-consuming, this point should already be addressed in step 1. Therefore, already as part of the fact-finding, the scope and adequacy of the **technical and organizational measures** (**TOM**) to ensure data security should be reviewed and documented. Whether further measures are necessary can usually only be assessed by taking into account the identified data categories, their purpose of use and the processing carried out.

The nDPO stipulates that the appropriateness of the TOM must be assessed on the basis of the **need for protection** (*Schutzbedarf*) regarding the data in question and the **risk** to the personality or fundamental rights of the data subjects, and contains guidance on how to proceed and which criteria to observe (Art. 1-5 nDPO).

7 Steps 2 and 3

Based on the preparation in step 1, **step 2** focuses on the **measures with external impact** and possible sanction consequences. This includes the following topics, which we will

address in the next newsletter:
- Duty to inform and data privacy notices
- Right to information (Data Subject Access Request (**DSAR**))
- Cross-border transfers, Transfer Impact Assessments (**TIA**) and Standard Contractual Clauses (**SCC**)

In **step 3**, the focus will be on **internal measures, processes and documents**, with prioritization of the areas sanctioned under the nDPA. We will thus address the following topics in the third newsletter:
- Processing agreements (outsourcing of data processing
- Automated individual decisions
- Professional secrecy obligation
- Internal data protection policy and employee training
- Data breach notification
- Data protection impact assessments (DPIA)
- Data portability
- Data retention and retention periods

8 Conclusion and Outlook

The implementation of the nDPA should not be taken lightly. In the event of violations of the new requirements, there is a threat of severe sanctions directed at the decision-takers. Implementation itself is no "rocket science", but does involve relevant effort and should be carefully planned and initiated promptly.

The actual implementation can be structured into three steps, related to **(1) preparatory measures**, **(2) implementation of external measures**, and **(3) implementation of internal measures**. We have outlined the first of these steps above, and we will address the need for action for the other two steps in two follow-up newsletters in the coming months.

Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch

Dr. Samuel Klaus
Partner Zurich
samuel.klaus@swlegal.ch

Vincent Carron
Partner Geneva
vincent.carron@swlegal.ch

Dr. Catherine Weniger
Counsel Geneva
catherine.weniger@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P. O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.ch

Geneva
15bis, rue des Alpes
P. O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.ch

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg