N

Monthly
Newsletter
December 2022

Schellenberg
Wittmer

Data

Implementation of the New Data Protection Act: Step 3 – Internal Measures

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

1.
The record of processing activities (RoPA) provides an overview of data processing and can serve as a central starting point for implementing the various measures.

2.
A general internal data protection policy is recommendable, in certain cases a specific processing policy may be mandatory, and employees should be trained accordingly.

3.
Responsibilities, processes, and templates should be defined for data protection impact assessments (DPIA), data breach notifications, and regarding automated individual decisions.

1 Overview

The new Data Protection Act (**nDPA**) and the new Data Protection Ordinance (**nDPO**) will come into force on 1 September 2023. In our October 2022 newsletter, we presented a **three-step roadmap** and set out the first step (preparation) in more detail. Step 2, focusing on measures with external effects, was covered in the November 2022 newsletter. Regarding **step 3** we now focus on the **internal measures** in the following areas:

- **Contracts and Policies** (outsourced processing, professional secrecy, data protection policy and trainings)
- **Operative Processes** (data protection impact assessment, data breach notifications, automated individual decisions)
- **Administrative / technical processes** (record of processing activities, data portability, retention period)

2 Contracts and Policies

2.1 Outsourced Processing

The nDPA introduces stricter requirements regarding situations where the controller outsources certain processing to an external processor: A **Data Processing Agreement** should be put in place to ensure that the processor processes data only in the same manner in which the controller is permitted to, and that no sub-processors are engaged without the controller's involvement. Therefore, appropriate rights of instruction and control as well as approval mechanisms must be provided for. Templates aimed at implementation under Art. 28 of the EU General Data Protection Regulation (**GDPR**) **meet the requirements of the nDPA**, provided their wording is adapted to Swiss law.

The above requirements **also apply to intra-group processing**, and some of the duties relating to outsourced processing are **now subject to a fine** under the nDPA. Existing Data Processing Agreements should therefore be reviewed, and compliance with the minimum requirements must be ensured when concluding new ones.

2.2 Professional Secrecy

The current law already qualifies the **violation of professional secrecy** a criminal offense, but it is limited to secret sensitive personal data and personality profiles (Art. 35 of the Federal Act on Data Protection). Under the nDPA, **all secret personal data** will be covered: Thus, the type of data is no longer relevant, but only whether it is "secret": the focus is on the fact that the person concerned has a (recognizable) interest in secrecy worthy of protection and the will to maintain such secrecy, provided the data is not already publicly known (or accessible). Anyone who intentionally discloses secret personal data can be punished under the nDPA with a **fine of up to CHF 250,000**.

If secret personal data is processed, it should be checked whether **specific provisions should be included in the customer contracts** (or in the contracts with other data subjects, in general terms and conditions, etc.). In any case, it is advisable to have internal guidelines on this topic and to sensitize employees.

2.3 Data Protection Policy and Trainings

Unlike the GDPR, the nDPA does not provide for a general accountability obligation. However, **to ensure data security**, suitable technical and organizational measures (**TOM**) must be implemented and documented accordingly. The nDPO contains further requirements in this regard, including the **obligation to implement a processing policy**: If sensitive personal data is processed automatically on a large scale or if high-risk profiling is carried out automatically, a processing policy with the **minimum content set out in Art. 5 nDPO** must be implemented. Intentional non-compliance with the provisions regarding minimum requirements can be sanctioned with a **fine of up to CHF 250,000**.

Even if the threshold for the obligation to create a special processing policy is not reached, a **general internal data protection policy** should be set up as part of TOM, specifying how personal data is processed internally, the applicable rules to be observed, and what the related responsibilities are. It is important that this guidance is actually put to practice: Employees must be made aware of their data protection obligations through appropriate **training and education**, and supported in their implementation. This is particularly advisable in view of the extended duty of professional secrecy (see above).

The outsourcing of processing activities requires specific contractual measures.

3 Operative Processes

3.1 Data Protection Impact Assessment (DPIA)

If new data processing is planned that may entail a high risk for the data subject, a **data protection impact assessment (DPIA)** must be carried out. A high risk may arise from the type, scope, circumstances and purpose of the data processing, in particular when using new technologies (such as artificial intelligence, **AI**). The DPIA serves to assess the associated risks and the implementation of risk mitigating measures (such as data minimization, anonymization, access restrictions, etc.).

The **scope and level of detail** of the DPIA depends on the complexity and risk profile of the planned processing. When carrying out the DPIA, representatives from the business side (regarding the factual questions) and from legal/compliance (regarding the data protection aspects) should work together closely. If the DPIA leads to the conclusion that even the planned mitigating measures cannot sufficiently limit the risk, the Federal Data Protection and Information Commissioner (**FDPIC**) must be consulted (or the internal data protection advisor, if one has been formally appointed) prior to implementing the planned data processing.

3.2 Data Breach Notifications

The nDPA introduces a **new obligation to notify data breaches**. If data security is breached (e.g. through loss of data, whether on paper or digitally, through unauthorized ac-

cess, etc.), the **FDPIC** must be informed if this breach is likely to result in a high risk for the data subjects. The nDPA does not provide for a specific time limit for the notification; however, it must be made **as soon as possible**, whereby one can find guidance in the 72-hour time limit according to the GDPR. The **data subjects** must be informed if it is necessary for their protection (e.g. because credit cards must be blocked or passwords changed) or if the FDPIC so requests.

To implement the notification obligation, **responsibilities and processes** should be defined so that it is clear who will take the relevant decisions, and according to which criteria, in the hectic period immediately after the discovery of a data breach, and how these decisions are then to be implemented. Although the notification obligation is (in contrast to the GDPR) not subject to a fine, its violation can lead to reputational damage (and possibly trigger an investigation by the FDPIC).

Additional statutory or contractual notification obligations should also be considered. It is often unclear, vis-à-vis which contractual partners such notification obligations exist. Therefore, a separate overview of such contractual notification obligations should be set up (and kept up to date) to ensure a quick reaction if necessary - also in order to avoid contractual liability consequences.

Under certain circumstances, a special processing policy must be implemented.

3.3 Automated Individual Decisions

Automated individual decisions (AID) are judgment decisions taken by an AI algorithm without human intervention and which have a relevant impact on the data subjects: for example, the automatic display of personalized advertising on a website is not an AID, but the purely AI-based rejection of a job application would be. AID are not very widespread yet, but their use will increase as digitization and automation progress.

If AID are used, additional requirements regarding the **duty to inform** as well as regarding the **privacy notice** must be observed, and **special consultation and review processes** must be provided for. To a certain part these obligations are **subject to a fine**. The use of AID should therefore be identified and addressed at an early stage (e.g. when new software with AID functions is being implemented).

4 Administrative / Technical Processes

4.1 Record of Processing Activities (RoPA)

We have already pointed out the importance of the **record of processing activities (RoPA)** in our newsletter of October 2022: The RoPA is the **central instrument for implementing the nDPA**, since the overview of the data processing activities can serve as the starting point for all further measures. Both the controller and the processor must generally keep a RoPA, whereas Art. 12 nDPA sets out different minimum content requirements for each.

However, there are no requirements regarding the **form and structure** of the RoPA. It is possible to use software solutions widely available on the market or - especially in simpler situations - to create one's own RoPA (e.g. in Word or Excel). It is helpful if the structure follows the **data processing carried out**, as this simplifies the direct use of the information for further measures. If the structure is based only on the technical aspects (e.g. the applications used), this may save some effort in the creation of the RoPA itself, but in the long term it might reduce the ease of handling and further use of the information contained therein.

4.2 Data Portability

Based on the obligation to ensure **data portability**, the controller must hand over to the data subjects the automatically processed personal data that **they themselves have disclosed** or that the controller has collected about them **when using a service** (e.g. an online service) **or device** (e.g. a fitness tracker). The data must be provided in a **common electronic format**. Data that the controller has itself generated from the collected data through its own evaluation (e.g. the individual user profile created from the collected data) does not have to be handed over.

For the disclosure of data to be feasible at all, it must be ensured that the personal data of a data subject can be **identified**, **isolated** from other data, and, if necessary, **migrated** into a common electronic format. The obligation to set up the systems and processes accordingly arises from the principle of **privacy by design** (Art. 7 nDPA).

New high-risk data processing will require a data protection impact assessment.

4.3 Retention Period

It follows from the **principle of data minimization** that data must be deleted when it is no longer required for the original purpose. Exceptions require justification, e.g. due to legal or contractual retention requirements or overriding interest of the controller (e.g., as long as the data may still have to be used in a possible legal dispute).

A **retention policy** should be implemented, setting out the retention period per data category and the steps necessary for deletion. It should also be ensured that such **deletion processes** are in fact implemented (e.g. by setting an "expiration date" for data files) and actually carried out (e.g. by setting up annual archiving and deletion routines).

5 Outlook and Conclusion

Particularly in regard to internally effective measures, the nDPA brings with it **relevant new obligations** that should not be taken lightly. Their implementation itself is not "rocket science", but it does entail an effort that should not be underestimated and should therefore be tackled promptly.

We have shown how the roadmap for implementation can look like in our newsletter of October 2022, and addressed the externally effective measures in our newsletter of November 2022. This newsletter on the internally effective measures hereby concludes our three-part series on the implementation of the nDPA.

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.com

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

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