SIDLEY

Swiss Data Protection Act

Part 1: Revised to Live Up to the Digital Age

Sabrine Schnyder

After three years of discussions, the Swiss parliament has agreed on the final draft bill of a new and modernized Swiss Data Protection Act (nDPA).

The Swiss government entered the legislative process with two main objectives: to enhance the level of protection of personal data provided in the current Swiss Data Protection Act (DPA) (largely, to align with the EU General Data Protection Regulation (GDPR)) and to ensure that there is an "adequate" level of data protection to allow for the continued flow of personal data from the European Economic Area (EEA) to Switzerland. The outcome is a modernized version of the existing DPA responding better to the needs of a digitalized world but without changing the law at its core.

Although the Swiss government has not formally set a date, it is expected that the nDPA (and the corresponding ordinance, which is still in the drafting process) will enter into force at the beginning of 2022. As the revised law does not in general provide for a grace period, businesses will have to comply with the new law at its entry into force. Hence, it is now a good time to start the process and make your business fit for the new law.

This article focuses on the provisions applicable to private controllers (as opposed to federal authorities) and provides an overview of the new obligations that will be imposed on controllers and processors and analyzes some key revisions in more detail. The second part, to be published in January 2021, focuses on some differences that exist between the nDPA and the GDPR and will provide businesses with an action plan.

WHAT IS NEW?

Revised Scope of Application

To respond to the ongoing globalization and international business activities, the legislator decided to equip the law with a broader territorial scope of application: The nDPA will apply to all processing of personal data that has an effect in Switzerland, irrespective of where the processing takes place; for example, it would apply to the processing of personal data of Swiss citizens by an entity located in France. Also, a company based outside Switzerland may have an obligation to appoint a representative (Article 14 nDPA). With regard to the material scope, the nDPA no longer applies to company data, whereas the nDPA's definition of "sensitive personal data" now also includes genetic data and biometric data. Finally, the nDPA differentiates between "profiling" and "high risk profiling," the latter defined as "profiling which involves a high risk to the personality or fundamental rights of the data subject, as it creates a pairing between data that enables an assessment of essential aspects of the personality of a natural person." The future will show where the regulator and courts will draw the line between "profiling" and "high risk profiling."

New duties imposed on controllers and processors

The nDPA imposes a plethora of new duties on controllers and, in some cases, on processors. While most of them are already known under the GDPR, businesses that are not yet compliant with the GDPR will face new obligations, such as these:

- ***The duty of information (Article 19 nDPA et seq.).*** Under the new law, the controller must inform the data subject about the collection of any personal data, not only sensitive data as was the case under the existing law. Thereby, the notice should include information about the transfer of the personal data outside of Switzerland and any automated decision making. While the nDPA does not impose any specific form requirements, publishing privacy policies on the company's website will in most cases present a convenient solution to this legal obligation, especially as they can easily be updated if necessary. In addition, it is worth mentioning that the notice must be provided to the data subject at the latest, within one month if the personal data is not collected directly from him or her and specific rules apply on automated decisions.

- ***The duty to keep an inventory (Article 12 nDPA).*** In the same spirit, the nDPA requires controllers and processors to maintain an inventory of processing activities — except for entities with fewer than 250 employees and whose processing entails only a low risk of infringing the personality rights of the data subjects. In this context, it is important to note that the new law now expressly states that personal data must be destroyed or anonymized as soon as it is no longer needed with regard to the purpose of the processing. Unfortunately, the law fails to provide further guidance on the timeframes. Hence, they will need to be set in accordance with legal recordkeeping obligations and the purpose of the processing.

- ***The duty to notify data security breaches (Article 24 nDPA).*** Another new important obligation under the nDPA is the controller's duty to notify the Federal Data Protection and Information Commissioner (FDPIC) of a personal data breach without undue delay where it is likely to result in a high risk to the rights of data subjects. Furthermore, the controllers must notify the data subject about a personal data breach if this is necessary for the safeguard of the data subject or if FDPIC so requests.

- ***Other new obligations:***

    - *Privacy by Default/Privacy by Design (Article 7 nDPA),* requiring controllers to consider data protection from the outset and, as a default, by processing a minimum of personal data.

- *Data protection impact assessment (DPIA, Article 22 nDPA),* requiring controllers to conduct a DPIA if the intended processing may lead to a high risk for the rights of data subjects.

- *The data subject's right to data portability (Article 28 nDPA),* that is, the right to access personal data or have this transferred to a third-party controller.

- *Codes of Conduct (Article 11 nDPA):* Supporting self-regulation, the new law allows professional, industry, and business associations to establish their own codes of conduct.

WHAT HAS BEEN REVISED?

Besides these new obligations, the legislature has revised some of the existing concepts, hopefully bringing more clarity in the future. While the content of these provisions has not changed at its core, the legislature has streamlined the wording, refined the language, and in some cases imposed new obligations or restrictions.

- ***Cross-border data transfers (Article 16 nDPA et seq.).*** Transfer of personal data from Switzerland abroad remains prohibited unless transfer is made to a country that provides an adequate level of protection of personal data (e.g., EU countries and the UK after Brexit). In the absence of an adequacy decision by the Federal Council (e.g., transfers to the United States or India), these contracts may serve as transfer mechanisms:

  - international treaties

  - standard contractual clauses (SCCs)

  - binding corporate rules (BCRs) (like SCCs, BCRs must be approved by the FDPIC; it is no longer sufficient to simply communicate them to the FDPIC)

  - data protection provisions included in a contract between the controller and the receiving party; as under the existing law, the controller must send a copy of these provisions to the FDPIC

  Other than on these contracts, the controller (or processor) may also rely on certain previously known exceptions to allow for the transfer of personal data from Switzerland to countries not deemed adequate:

  - Disclosure is necessary for the establishment, exercise, or enforcement of legal claims before a court or another competent foreign authority. While under the existing DPA, this exception was limited to courts, the broader wording under the nDPA, referring to courts and foreign authorities, is a

welcome change as it now also includes U.S. authorities, such as the Department of Justice or the Office of Foreign Assets Control. Before transferring personal data abroad, it is recommended to put in place confidentiality obligations, for example, by obtaining protective orders for U.S. pretrial discoveries. Also, one should keep in mind that Switzerland has blocking statutes that may prohibit the transfer of personal data abroad.

- Consent: In contrast to the current law, consent by the concerned data subject must be explicit under the nDPA.
- Close connection with the conclusion or performance of a contract with the concerned data subject or — new — a contracting partner in the interest of the data subject.

Finally, for some of these exceptions, the transfer must be notified to the FDPIC upon request.

- ***Outsourcing (Article 9 nDPA).*** While there is no change for controllers, the new law imposes additional restrictions on processors as they can no longer assign the processing to a third party without the prior authorization of the controller.
- ***Rights of access (Article 25 nDPA et seq.).*** Largely the same, but the nDPA specifies the type of information that must be provided to the data subject. The time limit to comply with this obligation is 30 days.

HOW IS THE NEW LAW ENFORCED?

Finally, the nDPA strengthens the rules on enforcement in case of noncompliance with its provisions.

First, FDPIC, the Swiss regulator, is vested with more power and the threshold to initiate an investigation has been lowered. Instead of issuing simple recommendations, the FDPIC will be entitled to open investigations on its proper initiative or upon complaint, order provisional measures, and render a binding decision (Article 51 nDPA). This means that the burden to appeal against binding decisions of the FDPIC now lies with the concerned controller (or processor). Also, the concerned controller (or processor) that is subject to an investigation by the FDPIC has a duty to cooperate. If it does not cooperate, the Swiss regulator may order requests for information, searches, witness examinations, and expert reports.

Second, the nDPA provides for higher sanctions, which are viewed as criminal sanctions, with fines of up to CHF 250,000 and new provisions on the liability of undertakings (Articles 60 nDPA et seq.). It's important to note that these criminal sanctions will be imposed on private individuals responsible for the breach and not the company as such. This will in most cases be the employee having effected the processing but can also be the management failing to set adequate internal safeguards against data breaches. Companies themselves may be subject to fines up to CHF 50,000 (Article 64 nDPA).

Third, the new law does not bring any substantial change with regard to private cause of action. Data subjects continue to have a right to rectification, a right to be forgotten, as well as a right to object to processing and may bring civil action in case of a violation of the rules set out under the nDPA.