SIDLEY

Swiss Data Protection Act

Part 2: Revised to Match the EU General Data Protection Regulation — or Almost

Sabrine Schnyder

It is fair to say that for the most part, the new Federal Data Protection Act (nDPA) does not go beyond the requirements of the European Union (EU) General Data Protection Regulation (GDPR), but the devil lies in the detail. The examples set out below illustrate where the nDPA and the GDPR differ.

General principle: The major difference between the nDPA and the GDPR lies in its approach: While under the GDPR, processing of personal data is unlawful unless there is a legal ground for such processing (Article 6 GDPR); the processing of personal data under the nDPA does not require reliance on such a legal ground and is lawful provided it is done in compliance with the principles stipulated in the law (Article 31 nDPA). Only where this is not possible, would the controller be required to identify a legal ground to justify such processing and these legal grounds are largely comparable with the grounds mentioned under Article 6 GDPR. In practice, this arguably more pragmatic approach is less burdensome for data controllers.

Scope of application: Although the GDPR has a very broad extra territorial scope, the nDPA's is broader as it applies to all processing of personal data that has "an effect in Switzerland" even if such processing takes place outside of Switzerland - for example, the processing of personal data of Swiss citizens by an entity located in the US. It should also be noted, that processing of personal data as part of Swiss court and arbitration proceedings will not be subject to the nDPA, as this is governed by the applicable Swiss procedural rules. This demonstrates once more the pragmatic approach the Swiss legislature has taken with regard to data protection.

Sensitive data: Unlike the GDPR, the definition of sensitive personal data includes data from administrative proceedings and social security measures, e.g. any measures taken by an authority for the protection of children and adults or a social security authority. This could be of importance when the salary of an employee is partially paid by invalidity insurance and the employer collects data on this arrangement. The nDPA also uses the term "data on the intimate sphere" which is arguably broader than its GDPR equivalent i.e., data concerning "a natural person's sex life or sexual orientation."

Personal data on children: The GDPR provides for specific rules on the processing of data of children i.e., in the context of offering them information society services. The nDPA does not

have a directly comparable provision and it is necessary to check the more general requirements in Swiss law on consent and legal age.

Right of access: Under both legislations, any person may request information from the data controller as to whether personal data concerning him or her is being processed i.e., the right of access. However, under the GDPR the data controller is obligated, in response to a request for access to personal data, to provide additional transparency information. The equivalent obligation does not exist under the nDPA. Further, under the nDPA, in order to restrict, refuse, or defer access to personal data, the controller must not have previously disclosed the relevant personal data to a third party. As such, to the extent a company has previously disclosed the personal data to e.g., an authority such as, Swissmedic, the company would not be able to rely on the exemption from complying with a request for access to personal data.

Professional Confidentiality Obligation (Article 62 nDPA): Under the nDPA there are specific criminal sanctions imposed on professionals that are willfully disclosing confidential personal data of which they have gained knowledge as part of their profession. Compared to Article 321a (4) of the Swiss Code of Obligations, which obliges employees not to disclose the employer's manufacturing or trade secrets, Article 62 nDPA protects the personal data of the customers. The provision is comparable with Article 321 of the Swiss Criminal Code sanctioning the violation of the professional secret, but applies to any professional processing personal data as part of its professional activity and not only to professionals bound by a professional secret, such as attorneys or doctors. This provision is extremely broad and would be something addressed at a national level under the GDPR.

Criminal sanctions: The nDPA differs from the GDPR by specifically providing for criminal sanctions instead of administrative sanctions. Criminal sanctions are imposed on the liable private individual (for example, the employee) and not the legal entity, and they are enforced by cantonal enforcement authorities and not the Federal Data Protection and Information Commissioner (FDPIC). By not vesting the FDPIC with the power to issue administrative sanctions against the concerned data controller, e.g., the company, the Swiss legislator has chosen a more complicated system by involving more authorities and parties in the process.

Outsourcing: The GDPR goes further in setting out the content of controller-processor (or processor-processor) agreements in more detail and requires that these agreements must be in writing. The nDPA does not have a form requirement for these so-called outsourcing agreements and requires less on the content. On the other hand, under the nDPA, outsourcing of the processing activities must not be prohibited by contractual or statutory confidentiality obligations. For example where a particular professional is bound to professional secrecy, this could prevent outsourcing of certain processing activities. Whether this exception applies must be analyzed on a case by case basis.

Data protection officer: Compared to the GDPR, appointment of a data protection officer remains optional for private controllers.

WHAT ACTION SHOULD COMPANIES TAKE?

The Federal Council has not yet set a date for the entry into force of the nDPA as this depends on how fast the Federal Council can issue the ordinance to the nDPA (regulating certain provisions in more detail). Although, it is expected the nDPA will apply as of the beginning of 2022. However, experience with the GDPR has shown that implementation of the new obligations under the nDPA will take time and resources. Therefore, companies are well advised to consider the following actions:

- data mapping to identify the flows of personal data and the processing activities carried out;
- establishing internal policies and guidelines on, for example, how to respond to information requests or when to notify personal data breaches. Personnel should also be trained on these requirements;
- updating security measures; while it is now an obligation to notify personal data breaches in certain circumstances, it has become even more important to try and prevent them and in turn, protect the company from potential financial and reputational damage;
- reviewing outsourcing and data transfer agreements for compliance with the new requirements of the nDPA. The review should also take into consideration (as necessary) recent developments on international transfers i.e., following the landmark decision of the Court of Justice of the European Union (CJEU) in Schrems II. In this case, the CJEU invalidated the EU-US Privacy shield, which was used by many companies as the legal transfer mechanism to transfer data from the EU to the United States, and determined that companies transferring personal data outside of the EEA in reliance on Standard Contractual Clauses (SCCs) should carry out an assessment as to whether the recipient country is "essentially equivalent" to the EU from a data protection perspective. Even though Schrems II is not directly applicable to companies in Switzerland i.e., unless they are subject to the GDPR, the FDPIC recently concluded in a position paper published on 8 September that the Swiss-US Privacy Shield no longer provides a valid mechanism for the transfer of personal data from Switzerland to the US. Further, it is expected that the Swiss regulator will approve the revised SCCs (published in draft by the European Commission to address the Schrems II decision).