SIDLEY

Swiss Data Protection Act

New Guidance by the Swiss Regulator

William Long, Francesca Blythe, Sabrine Schnyder

On March 5, 2021, the Swiss Federal Data Protection and Information Commissioner (FDPIC) published a position paper on the revised Swiss Data Protection Act (revDPA). The revDPA will implement many of the requirements of the EU General Data Protection Regulation (GDPR) into Swiss law, although sometimes with a Swiss finish. To quote the FDPIC, "The new [revDPA] is in line with Switzerland's legal tradition, as it features a high level of abstraction and is technology-neutral. It sets itself apart from the GDPR not only in its brevity, but also in the sometimes different terminology it uses."

Personal data of natural persons

It will come as a relief to many that in terms of material scope, the revDPA is aligned with the GDPR and will no longer protect personal data of legal entities, such as commercial organizations, associations, and foundations. However, legal entities can continue to seek protection of their privacy under Article 28 of the Swiss Civil Code, and manufacturing and trade secrecy remains protected under Article 162 of the Swiss Criminal Code, as well as under the Federal Act against Unfair Competition and the Federal Act on Cartels and other Restraints of Competition.

Cross-border data transfers

Unfortunately, the FDPIC does not provide guidance with respect to the aftermath of the *Schrems II* decision, although the FDPIC confirmed in an earlier position paper, dated September 8, 2020, that the Swiss-U.S. Privacy Shield does not provide an adequate level of protection for the transfer of personal data from Switzerland to the United States.

To date, the FDPIC has not provided any guidance as to what extent existing standard contractual clauses (SCCs) must be adapted and/or supplemented with additional safeguards. However, the FDPIC confirms that it will recognize SCCs that have been approved by the European Commission under the GDPR, which will likely include the revised SCCs expected to be published shortly by the European Commission. In turn, the question arises whether the FDPIC will continue to accept the previous versions of EU SCCs or whether companies will be forced to adapt the SCCs and transfer agreements they are currently using.

Obligation to report personal data breaches

Pursuant to Article 24 of the revDPA, the controller must notify certain serious personal data breaches to the FDPIC "as soon as possible." The FDPIC notes that "controllers should have previously drawn up a prediction of the potential implications of the breach and carried out an initial assessment as to whether there could be an imminent danger, whether data subjects need to be notified and how this could be done." In turn, controllers are not required under the revDPA to inform the FDPIC about unsuccessful cyberattacks, although voluntary reports may be submitted to the FDPIC.

Data protection officers (DPO)

The revDPA expressly provides for the possibility to appoint a DPO (Article 10 of the revDPA). Unlike under the GDPR, the designation of a DPO is always optional for private controllers. In its guidance (and in line with the GDPR), the FDPIC emphasizes the importance of the independence of a DPO, meaning that his or her activities should remain separate from other business activities of the controller, including other legal advice and representation. Notably, where a DPO has been appointed there would be no need for a company to consult with the FDPIC in the event the outcome of a data protection impact assessment identifies a high risk for data subjects. In such case, consultation with the DPO is sufficient. Moreover, as opinions of the FDPIC can be accessed under the Freedom of Information Act, protecting business secrets may present another incentive to designate a DPO.

Data protection impact assessments (DPIA)

Pursuant to Article 22 of the revDPA, not only federal bodies (as was the case under the current law) but also private controllers will be obliged to conduct a DPIA prior to a processing that presents a high risk. According to the FDPIC (and in line with the GDPR), "the high risk comes from the nature, scope, context and purposes of processing — particularly when using new technologies. In particular, processing is deemed high risk if profiling or extensive processing of sensitive data is planned."

Sanctions

An important difference between the revDPA and the GDPR is the applied sanction regime under the revDPA. In case of an intentional violation of the revDPA, private individuals (and not the company) may face criminal sanctions up to CHF 250,000 (Article 54 of the revDPA). In addition, companies may be sanctioned with a fine not exceeding CHF 50,000 if it is not possible to identify the responsible private individual within the company. Unlike under the GDPR, it is not the FDPIC that can impose these fines. These powers remain with the cantonal criminal prosecution authorities. The FDPIC can simply report to these authorities the noncompliance with the revDPA that it considers should be subject to a fine. The future will show how these authorities will work together and how these fines will be applied.

The role of the FDPIC

The revDPA vests new powers to the FDPIC: It will now investigate all violations of the revDPA except minor breaches (Article 49 of the revDPA). The FDPIC confirms, however, that a controller can prevent formal sanctions if he or she recognizes and rectifies the deficiencies in the application of the law within a reasonable time period after being notified by the FDPIC. Interestingly, the FDPIC confirms that it will continue to prioritize investigations according to the principle of discretionary prosecution due to its limited resources. Moreover, the FDPIC now has the power to issue binding decisions — which a concerned controller could appeal. The FDPIC may order a controller to delete personal data or even adapt, suspend, or discontinue its processing activity including to send specific notices to data subjects.

Fees

The FDPIC will now charge a controller additional fees to, for example, issue opinions on DPIAs and codes of conduct and the approval of standard data protection clauses. Also, the FDPIC states that it will no longer consult private controllers for free.

In addition to the above, the FDPIC also commented on the duty to provide privacy notices, the rights of data subjects, the principles of privacy by design (data protection through technology design), and privacy by default (only data that is absolutely necessary to a specific purpose is processed) as well as data portability, certifications, and the obligations to keep records on the processing activities.

The position paper is available on the FDPIC's webpage.