Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Federal Data Protection
and Information Commissioner (FDPIC)

Switzerland's new data protection law's changes impacting business

Privacy Laws & Business
33rd Annual International Conference

Monday, 23 November 2020

Urs Maurer-Lambrou
Delegate for International Affairs FDPIC

Overview

I. Why a law revision?

II. Introduction: Improving data protection

III. Where do we stand with the law revision process?

IV. What businesses must know in a nutshell

V. Various current issues

I. Why a law revision?

- Current FLDP dates from 16 June 1992:
  Modern generation law, technologically neutral

- Anyway, there was a need to strengthen data protection law

- In Europe, the GDPR with far-reaching changes was enacted

- Council of Europe Convention 108 was updated (Convention 108+) and is open for signature and ratification

- Ensuring that Switzerland continues to be recognized as a country with an adequate level of data law

II. Introduction
Improving data protection

- Improved transparency in data processing
- Improving the control of individuals over their data
- Precise definition and extension of the duties of the responsible persons
- Strengthening the powers of the Federal Data Protection Commissioner
- Extension of civil and criminal sanctions

III. Where do we stand with the law revision process?

- September 2017: Publication of the draft law by the Federal Council (government).
- About 3 years of parliamentary review & debates. Final law passed by parliament in September 2020.
- Entry into force? There is still some uncertainty. The Federal Office of Justice must draft the ordinances followed by a public consultation.
  Enactment early 2022 or June 2022?

IV. What businesses have to know in a nutshell (I)

- Territorial scope: impact principle
- New information and documentation requirements
- Data portability
- Data protection by design & by default
- Data protection advisor (voluntary)
- Codes of conduct (may be submitted to FDPIC for opinion)
- Appointment of representative in Switzerland (limited scope)

IV. What businesses have to know in a nutshell (II)

- Cross-border disclosure (stricter)
- Data protection impact assessment
- Duty to report data loss and other security breaches
- Risks of fines and criminal liability (also personal liability)
- Legal persons are no longer covered by the law

Good to know - revised FDLP generally not stricter than GDPR, but nevertheless not identical.

Territorial scope: Impact Principle

- The FDPL is applicable to fact patterns that have an effect in Switzerland, even if they occurred abroad.

- The FDPL is applicable if a sufficient connection to Switzerland is established. It is sufficient that the affected persons are in Switzerland and therefore a relevant impact in Switzerland occurs, but the data processing is carried out abroad and the person responsible for the data also does not have its registered office in Switzerland.

This provision of Art. 3 para. 1 FDPL thus goes beyond Art. 3 para. 2 GDPR.

New information & documentation requirements

- The new FLDP extends the duty to inform the data subject in the data collection process.
- According to Art. 12 FDPL, every controller and processor must keep a record of the inventory of their processing activities, like the GDPR provisions.
- Exceptions for inventory lists may apply (to be specified in the future by the Federal Council in the ordinance)

Data portability

- The right of “data portability” was newly introduced in the parliamentary consultations.

- It is more of a consumer protection measure and intends to give users the right to their data to contributions, pictures, followers, friends etc. in order to more easily switch to the competition.

Data protection by design & by default

- “Privacy by design” was already known under the current law, but not explicitly mentioned.

- “Privacy by default”: this concept is new in the FDPL.

Data protection advisor

- The appointment of a data protection consultant is voluntary.
- If you process data with “high risks” and have appointed a data protection consultant, you do not need to submit your project to the FDPIC.
- The data protection consultant must check the project instead of the FDPIC.

Codes of conduct

- Code of conducts are now regulated in the new FDPL.
- A code of conduct can, but does not have to, be submitted to the FDPIC.
- If a code of conduct is presented to the FDPIC, he must state his position on it.

Appointment of representative in Switzerland

The appointment of a representative in Switzerland is only necessary if the organization processes personal data of persons in Switzerland and the data processing fulfills the following requirements:

a. The data processing is connected to offering goods or services in Switzerland or to monitoring the behavior of these persons.

b. The processing is extensive.

c. It is regular processing.

d. The processing involves a high risk for the personality of the data subjects.

Cross-border Disclosure (stricter)

- In principle, not much will change with the new FLDP.
- Now it is no longer the data exporter who must assess whether a third country offers an adequate level of data protection, or not. This is decided instead by the Federal Council authoritatively (of course subject to judicial review, similar to the way the European Commission does it).
- It will be more a political issue with possible judicial review.
- Currently, the FDPIC publishes a white list with countries with adequate protection. However, this list is not binding, and the data exporter is always responsible for any transfer.

Data protection impact assessment

- “Data protection impact assessment”: If the intended data processing may lead to a high risk for the data subject’s personality or fundamental rights, the controller must beforehand conduct a data protection impact assessment.

- If a high risk is at issue, the project must be submitted to the FDPIC for consultation. He has three months to evaluate and, if necessary, suggests further measures or the termination of the exercise.

Duty to report data loss and other security breaches

- A loss of data or another data security incident, must under certain circumstances be reported to the FDPIC.

- Such data security breaches must only be reported if there is a “high risk” of negative consequences for the person concerned.

- The controller shall also inform the data subject if this is necessary for the protection of the data subject or if the FDPIC so requests

Risks of fines and criminal liability

- Breach of obligations to provide access and information or to co-operate (fines of up to CHF 250’000).
- Violation of duties of diligence (fines of up to CHF 250’000)
- Breach of professional confidentiality (fines of up to CHF 250’000)
- Disregard of decisions of the FDPIC (fines of up to CHF 250’000)

Legal persons are no longer covered by the law

End of a long tradition in Swiss civil law, that legal persons have generally the same rights as natural persons.

V. Various current issues

- Schrems 2
- Brexit
- EU adequacy decision

Thank you for your attention!

Q&A section…

I will gladly answer your questions now, or you may also contact me later at your convenience