Status update on Swiss legislation

Swiss Chapter CSA Event

Status update on Swiss legislation

Topics

- Public consultation notification obligation for cyberattacks on critical infrastructures – Amendment to the Information Security Act
- Revised Federal Act on Data Protection (FADP)
- Online identification for the e-signature possible
- Applicability of official secrecy (Article 320 SCC) to IT providers
- Protect our SMEs

Notification obligation for cyberattacks on critical infrastructures

- Federal Information Security Act (ISA) is not yet in force, the Federal Council is already proposing an amendment.
- The public consultation will last until 14 April 2022
- The proposal seeks to establish a legal basis for the notification obligation for cyberattacks and defines the tasks of the National Cybersecurity Centre (NCSC)
- The reporting requirements would also affect Cloud Providers, as "digital service providers" will fall within the scope of "operators of critical infrastructures"
- Digital service providers are companies that offer services on the Internet that (i) are used by a large number of users in Switzerland, (ii) are of great importance for the digital economy, or (iii) include security and trust services.
- Analogous to corresponding EU NIS Directive
- **According to the NIS Directive, only incidents with substantial impact must be reported. The proposed ISA amendment seems to be broader**
- Additional Information: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-86768.html

Revised Federal Act on Data Protection (FADP)

- Revised FADP enters into force on September 1st 2023
- The delay is mainly due to the wide disapproval of the draft of the Ordinance to the Federal Act on Data Protection
- Numerous provisions lack a legal basis or even directly contradict the will of the legislator (especially with regard to the documentation obligations newly introduced in numerous places).
- For instance, processing regulations are still in the draft version
- Technical and organizational measures in its core stay similar. However, are reference to Confidentiality, Integrity and Availability (CIA) is missing

Online identification for the e-signature possible

- Online identification for Qualified Electronic Signatures
- During Covid online identification for QES was already temporary possible
- ETSI has recently published the specification ETSI TS 119 461, which clarifies the requirements for identity verification performed by the service provider in the presence of the person to be identified or at a distance
- The Federal Office of Communications (OFCOM) has adapted the technical regulation in Switzerland. Since March, it is also possible in Switzerland to identify a person remotely

Applicability of official secrecy (Article 320 SCC) to IT providers

- Closing a gap to enable the use of external providers (e.g., Cloud Services) – auxiliary persons
- Currently no criminal liabilities; only contractual obligations/penalties
- However, the parliament had been of the opinion that this current law was incomplete and had therefore amended the article 320 SCC referred to. This revision is to come into force in 2023 together with the ISA, and, as Keller-Sutter recently emphasized, will also apply to ICT service providers abroad.
- It remains unclear on how to enforce it abroad

Breach official secrecy (320 SCC)

1. Any person who discloses secret information that has been confided to him in his capacity as a member of an authority or as a public official or as an assistant of a public official shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.

A breach official secrecy remains an offence following termination of employment as a member of an authority or as a public official or service relationship or the auxiliary activity has ended.

2. The offender is not liable to any penalty if he has disclosed the secret information with the written consent of his superior authority.

Protect our SMEs

- Motion: Protect our SMEs and public administrations from cyber attacks. This motion instructs the Federal Council to extend the Confederation's protection against cyber-attacks to the cantons, municipalities and the SME sector.
- The Federal Council requests that the motion be rejected, pointing out that, taking into account the principle of subsidiarity, responsibility for protection against cyber-attacks cannot be transferred to the Confederation and must remain with the authorities and SMEs themselves.

Overview Parliament (spring session)

Summary of the current IT topcis in the spring session:

https://www.lauxlawyers.ch/en/it-law-in-the-spring-session-2022/

Contact

LAUX LAWYERS AG
ZURICH | BASEL

Yves Gogniat

MA HSG, LL.M., Attorney-at-law, Advisor

@ yves.gogniat@lauxlawyers.ch

w www.lauxlawyers.ch

N linkedin.com/in/yvesgogniat

LAUX LAWYERS AG

Schiffbaustrasse 10
P.O. Box
CH–8031 Zurich
+41 44 880 24 24