# Data protection

Cybersecurity – challenges for political Switzerland

## State of the art

With increasing digitalisation, more and more data is being produced that can be misused for criminal purposes such as targeted attacks. Data protection is therefore becoming increasingly important. The safeguarding of personal privacy stands at the heart of data protection: protect our data and we protect our privacy too. Cybersecurity and data protection go hand in hand. Without adequate measures, unauthorised persons can penetrate systems and gain access to data, which means data protection is no longer guaranteed. That is why it is important to view cybersecurity as an integral part of data protection.

The following legislation applies for Swiss data processors:

– New Swiss Federal Act on Data Protection (FADP): The completely revised FADP is currently being debated in the National Council and the Council of States. The Act is expected to enter into force in 2021. The current Swiss Federal Act on Data Protection entered into force in 1992. A complete revision was necessary, firstly to keep pace with modern data processing methods, and secondly because the European General Data Protection Regulation (GDPR) – on which the completely revised Swiss legislation is to be based – has been in force since May 2018. Switzerland is aiming to establish equivalent and comparable data protection law.

## Recommendations

1. When drawing up the regulations, it is important to ensure that provisions and requirements are sufficiently precise, so that data protection can be implemented by means of effective measures.
2. The inter-cantonal harmonisation of data protection should be promoted.
3. The Federal Government should set up research programmes in the field of systematic control and traceability of data processing and data flows (e.g. via the Swiss National Science Foundation SNSF).
4. Definition and continual updating of minimum standards and good practices on anonymisation and pseudonymisation by the Federal Data Protection and Information Commissioner (FDPIC).

– EU General Data Protection Regulation (GDPR): This defines the duty of care for data processors and applies to Swiss companies providing goods or services in the European Economic Area (EEA).

There are lots of developments under way worldwide in relation to data protection regulations. Many countries are pursuing an approach comparable with the GDPR or one based on US legislation which focuses on IT security.

## Challenges

Granting people partial control and access to their own personal data is a resolvable problem. It is more challenging to control the data flow, process the data and maintain an implicit or explicit purpose for data usage once it has been released. Measures should be taken to ensure that data flows and data manipulations can be subsequently analysed and that areas of responsibility are clear and cannot be manipulated. In this respect, efforts should be made to provide the persons concerned with a degree of control over their own personal data.

The systematic control and traceability of data flows and processing of personal data across numerous organisations or units has at best only been partially resolved today.

The anonymisation and pseudonymisation of personal data are not trivial matters and the established methods do not always provide sufficient protection of the confidentiality or integrity of the data.

## Need for action

Data-processing organisations should practise appropriate and systematic data protection management (DPM) as an organisational and procedural basis for implementing data protection. In practice, fundamental security measures are often being implemented incompletely or ineffectively.

The systematic control and traceability of data processing and data flows require further research and development work.

To meet legal data protection requirements (Switzerland and EU) long-term, minimum standards and good practices should be defined for anonymisation and pseudonymisation and updated on an ongoing basis to keep pace with the development of analysis methods and solutions.

## References


- Swiss Federal Act on Data Protection: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html
- Swiss Ordinance to the Federal Act on Data Protection: https://www.admin.ch/opc/en/classified-compilation/19930159/index.html
- Swiss Ordinance on Data Protection Certification: https://www.admin.ch/opc/en/classified-compilation/20071826/index.html

Data protection Canton Zurich: http://dsb.zh.ch

- Swiss Federal Data Protection and Information Commissioner: https://www.edoeb.admin.ch/edoeb/en/home.html
- GDPR: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02016R0679-20160504
- Anonymisation/pseudonymisation: How common methods of data anonymisation are failing: http://www.heise.de/-4624450
- The ineffectiveness of data anonymisation: http://www.heise.de/-4479968


## Contact


Nicole Wettstein
Head of priority programme Cybersecurity
+41 44 226 50 13


https://www.satw.ch/cybersecurity-challenges


**Impressum**
Swiss Academy of Engineering Sciences SATW
**Expert contributions**
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
**Editing and graphics**
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein




www.satw.ch
**September 2020**