

# Datenschutz

Cybersecurity – Herausforderungen für die politische Schweiz



## Stand der Dinge

Mit der zunehmenden Digitalisierung werden immer mehr Daten produziert, die u.a. für kriminelle Zwecke, wie beispielsweise gezielte Attacken, missbraucht werden können. Dadurch kommt dem Schutz der Daten eine immer grössere Bedeutung zu. Beim Datenschutz steht der Schutz der Persönlichkeit im Zentrum, der Schutz der Daten ist das entsprechende Mittel dazu. Cybersicherheit und Datenschutz gehen Hand in Hand. Ohne adäquate Massnahmen ist es für Unbefugte möglich, in die Systeme einzudringen und Zugriff auf Daten zu erlangen, so dass der Datenschutz nicht mehr gewährleistet ist. Es ist somit zentral, Cybersicherheit als Teil des Datenschutzes zu verstehen.

Für Schweizer Datenverarbeiter gelten folgende Gesetzgebungen:

– Neues **Schweizerisches Datenschutzgesetz** (DSG): Das totalrevidierte DSG wurde in der Herbstsession 2020 von National- und Ständerat angenommen. Es wird erwartet, dass das Gesetz per 2021 in Kraft gesetzt wird. Das schweizerische Datenschutzgesetz ist seit 1992 in Kraft. Eine Totalrevision wurde einerseits aus Gründen der Anpassung an moderne Datenverarbeitungsmethoden nötig. Andererseits ist mit der europäischen DSGVO seit Mai 2018 eine Verordnung in Kraft, an die sich die totalrevidierte Schweizer Gesetzgebung anlehnen soll: Die Schweiz strebt ein äquivalentes und vergleichbares Datenschutzrecht an.

## Empfehlungen

1. Bei der Ausarbeitung der Verordnung ist auf ausreichend präzise Vorgaben und Anforderungen zu achten, so dass der Datenschutz mittels wirkungsvoller Massnahmen umgesetzt wird.
2. Die interkantonale Harmonisierung des Datenschutzes soll gefördert werden.
3. Der Bund soll Forschungsprogramme im Bereich systematische Kontrolle und Nachvollziehbarkeit von Datenbearbeitungen und Datenflüssen aufsetzen (z.B. via SNF).
4. Definition und kontinuierliche Pflege von Minimalstandards und Good Practices für Anonymisierung und Pseudonymisierung durch den Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB).

– **EU-Datenschutz-Grundverordnung** (DSGVO oder GDPR): Definiert Sorgfaltspflicht für Datenverarbeiter und betrifft Schweizer Unternehmen, sofern sie Waren oder Dienstleistungen im Europäischen Wirtschaftsraum (EWR) anbieten.

Weltweit gibt es viel Bewegung was Regulierungen im Datenschutz-Umfeld betrifft. Viele Länder verfolgen entweder einen mit GDPR vergleichbaren Ansatz oder einen an die US-Gesetzgebung angelehnten Ansatz, der auf IT-Sicherheit fokussiert.

## Herausforderungen

Betroffenen Personen die teilweise Kontrolle und den Zugang zu den eigenen Personendaten zu gewähren, ist ein lösbares Problem. Schwieriger wird es bei der Kontrolle von Datenfluss, Datenbearbeitung und der Beibehaltung einer impliziten oder expliziten Zweckbindung der Datennutzung im Anschluss an die Freigabe. Es sollte sichergestellt werden, dass Datenflüsse und Manipulation von Daten nachträglich analysiert werden können und Verantwortlichkeiten nachvollziehbar und nicht manipulierbar sind. In diesem Sinne ist anzustreben, dass betroffenen Personen eine gewisse Kontrolle über ihre eigenen personenbezogenen Daten ermöglicht wird.

## Handlungsbedarf

Datenverarbeitende Organisationen sollten ein angemessenes und systematisches Datenschutz-Management (DSMS) betreiben – als aufbau- und ablauforganisatorische Basis zur Umsetzung des Datenschutzes. In der Praxis werden bereits fundamentale Sicherheitsmassnahmen oft nur unvollständig oder ineffektiv umgesetzt.

Die systematische Kontrolle und Nachvollziehbarkeit von Datenbearbeitungen und

Die systematische Kontrolle und Nachvollziehbarkeit von Datenflüssen und Datenbearbeitung personenbezogener Daten über mehrere Organisationen bzw. Stationen hinweg ist heute höchstens teilweise gelöst.

Anonymisierung und Pseudonymisierung von personenbezogenen Daten sind nicht trivial und die bekannten Methoden bieten nicht immer genügenden Schutz der Vertraulichkeit oder Integrität der Daten.

Datenflüssen Bedarf weiterer Forschungs- und Entwicklungsarbeiten.

Um die datenschutzgesetzlichen Anforderungen (Schweiz und EU) nachhaltig zu erfüllen, sind für Anonymisierung und Pseudonymisierung Minimalstandards und Good Practices zu definieren und kontinuierlich der Entwicklung der Analysemethoden und -lösungen anzupassen.

## Referenzen

DSG Schweiz:  
<https://www.admin.ch/opc/de/classified-compilation/19920153/index.html>

VDSG Schweiz:  
<https://www.admin.ch/opc/de/classified-compilation/19930159/index.html>

VDSZ Schweiz:  
<https://www.admin.ch/opc/de/classified-compilation/20071826/index.html>

DSB Kanton Zürich: <http://dsb.zh.ch>

EDÖB Schweiz:  
<https://www.edoeb.admin.ch/edoeb/de/home.html>  
GDPR / DSGVO: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02016R0679-20160504>

Anonymisierung/Pseudonymisierung: Wie gängige Methoden zur Anonymisierung von Daten versagen:  
<http://www.heise.de/-4624450>

So wenig nützt Daten-Anonymisierung:  
<http://www.heise.de/-4479968>

## Kontakt

Nicole Wettstein  
Leiterin Schwerpunktprogramm Cybersecurity  
+41 44 226 50 13



<https://www.satw.ch/cybersecurity-herausforderungen>

## Impressum

Schweizerische Akademie der Technischen Wissenschaften SATW

### Expertenbeiträge

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, Verwaltungsrat und Berater | 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

### Redaktion und Grafik

Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

Die hier geäusserten Ansichten sind diejenigen der obengenannten Mitglieder des SATW Advisory Board Cybersecurity und spiegeln nicht unbedingt die offizielle Position der SATW und ihrer Mitglieder wider.

[www.satw.ch](http://www.satw.ch)

September 2020