Cyber Incident Response and Data Breach Notification (Switzerland)

by Jürg Schneider and Hugh Reeves, Walder Wyss Ltd., with Practical Law
Law stated as of 26 Mar 2020 • Switzerland

A Practice Note addressing legal requirements and considerations when handling data breaches, cyberattacks, or other information security incidents in Switzerland or drafting data breach response notifications regarding personal data originating from Switzerland. The Switzerland-specific guidance in this Note may be used with the generally applicable resources listed in the Global Cyber Incident Response and Data Breach Notification Toolkit.

Data breaches, cyberattacks, and other information security incidents are increasingly common across sectors and affect a wide range of large and small organizations. In response, data breach notification laws, regulations, and best practices raise significant challenges for global companies. This Practice Note explains the Swiss laws and regulations an organization must consider and the local resources available when handling data breaches of personal data originating from Switzerland.

Cyber incidents occur when events compromise the security, confidentiality, integrity, or availability of an information technology (IT) system, network, or data. Reporting and notification obligations vary according to a cyber incident's characteristics. For example:

- Data breach notification obligations may apply if the event exposes personal information to potential unauthorized access or use.
- Other cyber incident notification requirements may apply if the event affects critical infrastructure or regulated entities.

Some cyber incidents result from criminal activities. Victimized organizations should consider reporting cybercrime to applicable authorities.

The Switzerland-specific guidance in this Note may be used with the generally applicable resources listed in the Global Cyber Incident Response and Data Breach Notification Toolkit.

Data Breach Notification

Switzerland does not currently mandate general data breach notification for breaches of personal information. However, several laws, including the Federal Act on Data Protection (FADP), protect personal information in a way that implies a duty to prevent unauthorized disclosures. Swiss law also imposes sector-specific data security obligations on:

- Financial services organizations.
- Telecommunications providers.
- Healthcare providers and medical researchers.

On September 15, 2017, the Swiss Federal Council published the draft of a revised Federal Act on Data Protection that aims to:

- Adapt data protection laws with the internet age.
- Align Swiss law with the EU General Data Protection Regulation (Regulation (EU) 2016/679).
- Maintain Switzerland's adequacy status granted by the European Commission to ensure the free flow of personal data between the EU and Switzerland.

The revised FADP will replace the current FADP. The legislative review process continues. The Federal Council split the revision into two separate packages, specifically:

- The first part entered into force on March 1, 2019 and implemented some international requirements under the Schengen/Dublin framework, which addresses certain issues regarding migration and asylum.
- The second part comprises the main text of the draft revised FADP. It is still under discussion and not expected to enter into force before 2022. The current draft contains a data breach reporting obligation.

For more details on Switzerland's information security requirements, see Practice Note, Information Security Considerations (Switzerland).

Depending on the circumstances, organizations should consider voluntarily notifying affected individuals if a breach of personal data occurs because:

- Timely notification to affected individuals helps them to mitigate potential harm associated with any loss or misuse of their personal information.
- Notifying individuals and helping them protect themselves may decrease the risks of litigation and loss of customer trust that often occur following a data breach. For best practices in responding to global data breaches, see Practice Note, Challenges and Strategies for Handling Global Data Breaches: Overview.

Other Cyber Incident Notification Requirements

Switzerland does not require organizations to take any specific cyber incident response planning measures or provide any other incident notification. However, a robust, well-tested incident response plan can help organizations respond more effectively to these events (for an example plan, see Standard Document, Global Cyber Incident Response Plan (IRP)). Organizations that experience a cyberattack or other information security incident should consider:

- Reporting the event to any applicable authorities (see Reporting Cyberattacks and Cybercrime).
- Seeking assistance and sharing information through established computer emergency response teams or other cybersecurity information sharing programs (see Getting Help with Cyber Incident Response).

Enforcement and Litigation

Swiss law does not specifically empower any regulator to take enforcement actions against organizations that fail to implement and maintain reasonable security practices. However, the Data Protection Commissioner's office can investigate complaints:

- On its own initiative.
- At a third party's request, if the alleged violation may affect the privacy rights of many persons.

(Article 29, FADP.)

The law does not provide further guidance on what constitutes many persons. However, the Data Protection Commissioner is likely to investigate any complaint involving a serious risk of harm to data subjects, even if the number of affected subjects is relatively small.

If an organization refuses to comply with the Data Protection Commissioner's recommendations, the Data Protection Commissioner may refer the matter to the Federal Administrative Court for a decision (Article 29, FADP). Sector-specific regulators may also take enforcement action against organizations that fail to comply with security and risk management guidelines.

Data breaches and cyber incidents can trigger different administrative, civil, and criminal liabilities. Identifying the appropriate enforcement agency depends on the facts of the breach or other incident. However, organizations should always consider:

- Notifying the Computer Emergency Response Team of the Swiss Government (GovCERT) (see Getting Help with Cyber Incident Response).
- Reporting these events to authorities (see Reporting Cyberattacks and Cybercrime).

Getting Help with Cyber Incident Response

Switzerland supports public-private partnerships and various computer emergency response team (CERT) resources to coordinate cyber incident response and help organizations recognize, respond, and recover from cyberattacks. The Computer Emergency Response Team of the Swiss Government (GovCERT) coordinates computer security incident response for local businesses and internet users. For more details on information security and resources for preventing data breaches and other cyber incidents in Switzerland, see Practice Note, Information Security Considerations (Switzerland).

The Swiss Federal Council is working to establish a network of cybersecurity competence centers, under the national cybersecurity strategy. For more, see Practice Note, Information Security Considerations (Switzerland): National Strategies for Protection Against Cyber Risks.

Reporting Cyberattacks and Cybercrime

Title 2 of the Swiss Criminal Code recognizes several technology crimes, for example:

- Unauthorized obtaining of data, or unauthorized access to a data processing system (Article 143).
- Damage to data (Article 144).
- Computer fraud (Article 147).
- Obtaining personal data without authorization (Article 179).

These statutes cover criminal activities such as hacking, malware, and denial-of-service attacks. The Cybercrime Coordination Unit Switzerland (CYCO) combats illegal activities on the internet by:

- Serving as Switzerland's central office for reporting cybercrime.
- Analyzing reports and referring them to appropriate law enforcement agencies in Switzerland or abroad.
- Actively searching the internet for illegal subject matter.

