Cyber Incident Response and Data Breach Notification (Switzerland)

by **Jürg Schneider** and **Hugh Reeves**, Walder Wyss Ltd., with Practical Law Data Privacy Advisor

Practice notes | Law stated as of 07-Jul-2021 | 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 current 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 25, 2020, the Swiss Parliament adopted the Revised Federal Act on Data Protection (in German) (Revised FADP) that:

- Adapts data protection laws to the internet age.
- Aligns Swiss law with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), though some divergences remain.
- Seeks to 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 is expected to replace the current FADP in the second half of 2022.

Once in effect, the Revised FADP requires controllers to:

- Report data security breaches as soon as possible to the Federal Data Protection and Information Commissioner (FDPIC) if there is a high risk of adverse effects to data subjects' personality or fundamental rights (Article 24, Revised FADP). The report must identify:
    - the security breach type;
    - the breach's consequences; and
    - the measures the controller has taken or plans to take to address the breach.
- Notify affected data subjects if:
    - necessary for their protection; or
    - the FDPIC requests it.

Processors must notify applicable controllers as soon as possible of any data security breach.

(Article 24, Revised FADP.)

The FDPIC has issued a statement indicating that it expects organizations to consider, prior to submitting their notification under the Revised FADP:

- Whether there may be an imminent danger to data subjects.
- Whether they may need to notify affected data subjects of the breach.
- If necessary, how they plan to notify affected data subjects.

Like the GDPR, under the Revised FADP, controllers may:

- Use substitute notification if individual notifications are impossible or would require a disproportionate effort. Controllers in these circumstances should use a public communication or similar measure to inform affected individuals in an equally effective manner.
- Avoid individual notifications if:
    - necessary to protect a third parties' overriding interests or certain federal agency law enforcement or public security interests; or
    - a statutory duty of confidentiality prohibits it.

(Article 24(5), Revised FADP.)

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

Other Cyber Incident Notification Requirements

Switzerland does not have an overarching obligation requiring organizations to take any specific cyber incident response planning measures or provide any other incident notification. However, organizations should implement a robust, well-tested incident response plan to help them 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).
- In December 2020, the Swiss Federal Council initiated a legislative process that should result in a general duty on operators of critical infrastructure to report cyber incidents. The legislative process's timeline remains open, although observers expect Parliament to have a draft act ready by end of 2021.

Enforcement and Litigation

Current Swiss law does not specifically empower any regulator to take enforcement actions against organizations that fail to implement and maintain reasonable security practices. However, under the existing FADP the FDPIC 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 current law does not provide further guidance on what constitutes many persons. However, the FDPIC 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 its recommendations, the FDPIC may refer the matter to the Federal Administrative Court for a decision (Article 29, FADP).

The Revised FADP grants the FDPIC broader authority to conduct enforcement proceedings and take action against violators. For example, under the Revised FADP, the FDPIC can:

- Order data processing adjustments.
- Order controllers or processors to suspend or discontinue data processing.
- Order deletion or destruction of personal data.

The FDPIC's administrative powers under the Revised FADP allow it to require various measures, such as:

- Data security measures.
- Informing data subjects.
- Conducting impact assessments.
- Other required measures.

(Article 51, Revised 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), under the recently established National Cyber Security Centre (NCSC), 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 Federal Council has consolidated the network of cybersecurity competence centers under the NCSC to simplify nationwide coordination and enhance the speed and responsiveness of private-public interactions. 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 NCSC combats illegal activities on the internet through various activities, including:

- 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.

END OF DOCUMENT