Information Security Considerations (Switzerland)

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

A Practice Note describing the laws, regulations, enforcement practices, and local resources to consider when developing, implementing, and maintaining an information security program in Switzerland or as applied to data originating from Switzerland. It addresses requirements under the Federal Act on Data Protection (FADP), the Human Research Act (HRA), and circulars from the Financial Market Supervisory Authority (FINMA) and the Federal Office of Telecommunications (OFCOM). The Switzerland-specific guidance in this Note may be used with the generally applicable resources listed in the Global Information Security Toolkit.

Information security programs protect the confidentiality, integrity, and availability of data and information technology (IT) assets. However, differences in local data security laws, practices, and standards create challenges for global companies, and failure to comply with them can result in enforcement action and litigation. This Note explains the Swiss laws, regulations, enforcement practices, and local resources to consider when developing, implementing, and maintaining an information security program in Switzerland, or as applied to personal data originating from Switzerland.

The Switzerland-specific guidance in this Note may be used with the generally applicable resources listed in the Global Information Security Toolkit.

Information Security Laws and Regulations

Several Swiss laws regulate information security and set related standards, including:

- The Federal Act on Data Protection (FADP), which protects personal data (see Federal Act on Data Protection).
- Sector-specific laws and regulations, which impose further obligations on higher risk areas, such as financial services, telecommunications, and health care (see Sector-Specific Laws and Regulations).
- Other legal regimes that protect additional at-risk data, assets, and business interests (see Other Laws and Regulations).

Overall, Switzerland takes a flexible approach to information security. The laws generally grant organizations reasonable latitude to implement reasonable measures as they deem appropriate.

Federal Act on Data Protection

The FADP protects personal data using a principles-based approach and imposes data security obligations on all entities that process personal data, including private and public sector organizations. Personal data includes all information that relates to a natural or legal person (Article 3(a) and (b), FADP). For more information on the FADP's general requirements, see Country Q&A, Data Protection in Switzerland: Overview.

The Federal Data Protection and Information Commissioner (Data Protection Commissioner) enforces the FADP and provides detailed guidance on its website.

On September 15, 2017, the Swiss Federal Council published a draft 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.

Protecting Personal Data Under the FADP

The FADP's Principle of Data Security directs organizations to implement technical and organizational standards (Article 7, FADP). The Ordinance to the Federal Act on Data Protection (FADP Ordinance) further implements the FADP. The FADP Ordinance requires organizations to protect systems from:

- Unauthorized or accidental destruction.
- Accidental loss.
- Technical errors.
- Forgery.
- Theft.
- Other unauthorized processing.

(Article 8(1), FADP Ordinance.)

The technical and organizational measures must account for the:

- Purpose of the data processing.
- Nature and extent of the data processing.
- Possible risks to affected individuals, or data subjects.
- Commonly accepted practices.

(Section 8(2), FADP Ordinance.)

Special technical and organizational requirements apply to:

- Automated processing of personal data.
- Processing of sensitive personal data, which includes data relating to an individual's:
  - religious, political, or ideological views;
  - trade union activities;
  - health or intimate activities;
  - social security measures; or
  - criminal or administrative proceedings, including sanctions.
- Processing of personality profiles.

(Article 3, FADP.)

For example, organizations must:

- Ensure that their systems provide logging or other capabilities that permit reviews to determine who accessed data and when.
- Maintain a record of all automated processing of sensitive personal data.
- Grant only authorized personnel access to processing facilities and portable media that transport data.

(Articles 9 and 10, FADP Ordinance.)

The Data Protection Commissioner has issued guidelines on the minimum requirements for data protection management systems (DPMS) (available in French, German, and Italian on the Data Protection Commissioner's website. The DPMS guidelines incorporate widely adopted international standards for management systems, including the ISO 2700x series (see Industry Standards). IT managers should also consult the Federal Data Protection and Information Commissioner (FDPIC) Guide for Technical and Organizational Measures (FDPIC Technical Guide), which urges organizations to develop a data processing policy that addresses information security issues and provides detailed guidance on:

- Data access protective measures, including:
  - physical security for data centers and the workplace;
  - identification and authentication; and
  - external, or remote, access.
- Data lifecycle management controls, including:
  - data input;
  - logging;
  - pseudonymization and anonymization;
  - encryption;
  - security of storage media;
  - data backup;
  - data destruction;
  - outsourcing;
  - security and protection;
  - data transmission; and
  - right to information.
- Data exchange and transmission security, including:
  - network security;
  - message encryption;
  - digital signatures;
  - storage media handling;
  - data exchange logging; and
  - data subjects' rights.

Data Destruction under the FADP

The FADP's Principle of Good Faith and Proportionality requires organizations to retain personal data only as long as necessary to meet their stated objectives or fulfill legal obligations (Article 4(2), FADP). The Data Protection Commissioner advises organizations to implement reasonable security measures when destroying personal data. For example, organizations should:

- Develop policies that specify retention periods.
- Shred paper records.
- Physically destroy CD-ROMs and other online storage media.
- Use specialized software to permanently erase data on rewritable storage media.

(Section B.7, FDPIC Technical Guide.)

Sector-Specific Laws and Regulations

Swiss law imposes additional information security requirements in certain industry sectors considered higher risk, such as:

- Financial services (see Financial Services).
- Telecommunications (see Telecommunications).
- Health care and medical research (see Health Care and Medical Research).

Financial Services

The Financial Market Supervisory Authority (FINMA) monitors all financial markets under the:

- Mortgage Bond Act.
- Federal Act on Contracts of Insurance.
- Collective Investment Schemes Act.
- Banking Act.
- Stock Market Act.
- Financial Market Infrastructure Act.

(Article 1, Federal Act on the Swiss Financial Market Supervisory Authority (FINMASA).)

FINMA provides information security guidance in its Circular 2008/21 on Corporate Governance, Risk Management, and Internal Controls at Banks (available in German and French on the Financial Authority's website). The circular contains principles on proper risk management to ensure the confidentiality of electronically-stored client-identifying data (CID).

The Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (FMIA) requires central deposits, payment systems, and stock exchanges to implement IT systems capable of:

- Ensuring the availability, confidentiality, and integrity of data.
- Detecting and remedying security incidents.

(Articles 14 and 15, FMIA.)

Telecommunications

The Swiss Federal Council issues technical and administrative regulations to secure telecommunications services

under Article 48a of the Telecommunications Act (TCA). Service providers must immediately inform the Federal Office of Communications (OFCOM) of certain faults in the operation of their networks which affect customers (Article 96, Ordinance on Telecommunications Services).

OFCOM also recommends that providers develop an information security management system that aligns with the ISO 2700x information security standards (for more details, see Guidelines for Security and Availability of Telecommunication Infrastructures and Services (available in French and German) and Industry Standards).

Health Care and Medical Research

The Data Protection Commissioner recommends that healthcare professionals segregate client files from computers connected to the internet to help minimize data security risks (for more details, see Guidelines for Processing Personal Data in the Medical Field (available in French, German, and Italian)).

Swiss laws also require medical researchers to protect biological or health-related personal data. For example:

- The Federal Act on Research Involving Human Beings (HRA) requires users of health-related personal data to implement technical and organization measures to prevent unauthorized use (Article 43, HRA).
- The Human Research Ordinance on Human Research with the Exception of Clinical Trials (HRO) implements the HRA and requires users of health-related personal data to:
  - restrict access to health-related personal data;
  - prevent unauthorized disclosure, alteration, deletion, or copying of health-related personal data; and
  - document health-related personal data processing.

(Article 5, HRO.)

Other Laws and Regulations

Swiss law protects other types of at-risk data, assets, and business interests, including:

- **Public companies.** There are currently no specific data security requirements for listed companies. However, Article 20 of the Code of Best Practice for Corporate Governance requires companies to establish appropriate internal controls and risk management systems, considering the company's size, complexity, and risk profile. The Swiss stock exchange (SIX) also requires listed companies to implement internal auditing, risk management, and management information systems (Section 3.7, Annex, SIX Directive on Information Relating to Corporate Governance). The Swiss Code of Obligations (SCO) generally requires a company's board of directors to perform its duties with due diligence and safeguard the organization's interests in good faith, which reasonably includes applicable cybersecurity measures (Article 717, SCO).
- **Trade secrets.** Switzerland addresses trade secrets in its unfair competition and criminal laws (Article 6, Federal Act on Unfair Competition and Articles 162 and 273, Swiss Penal Code). To ensure trade secret protection, organizations should:
  - take sufficient organizational and technical measures to protect their information; and
  - execute non-disclosure agreements with third parties that have knowledge of the organization's trade secrets.
- **Business contracts.** Requirements to implement data security measures may also arise under contractual duties. Organizations that fail to support sufficient data security measures may be liable for damages claims based on Swiss contract, tort, and corporate law. Common obligation sources include:
  - data processing agreements;
  - non-disclosure agreements; and
  - general contractual commitments to follow industry standards and practices, including implicit or underwritten expectations.

National Strategies for Protection Against Cyber Risks

On April 18, 2018, the Swiss Federal Council adopted its national strategy for 2018-2022. The cyber strategy sets out seven priority areas, including:

- Researching and developing information regarding new cyber risks.
- Evaluating risks in existing systems and infrastructures.
- Analyzing the threat landscape.
- Building competences to address deficiencies in security management.
- Cooperating at the international security policy level.
- Improving resiliency and crisis management.
- Prioritizing amendments to existing legislation.

(Swiss Federal Council National Strategy for Switzerland's Protection Against Cyber Risks, at 4).

The Swiss Federal Council also updated its National Strategy for the Protection of Critical Infrastructure (available in German) on December 8, 2017.

Industry Standards

The ISO 2700x family of international information security standards, including ISO/IEC 27001 and ISO/IEC 27002, are widely adopted cybersecurity industry standards in Switzerland. Other commonly used industry standards include:

- British Standards Institute (BSI) PAS 555:2013, Cyber Security Risk – Governance and Management – Specification, which defines the outcomes required for effective cybersecurity and gives businesses the flexibility to choose technical standards and implementation approaches that fit their particular needs.
- COBIT 5, which provides a set of control objectives for enterprise IT governance and management that address information security issues.
- The Payment Card Industry Data Security Standard (PCI DSS), which applies to merchants and service providers that process payment card transactions or otherwise handle payment card data (see Practice Note, PCI DSS Compliance).

Adherence to these standards is not mandatory. However, organizations may voluntarily submit their systems for evaluation by recognized independent certification organizations (Article 11, FADP). The Ordinance on Data Protection Certification governs the accreditation process. Voluntary certification benefits the organization by:

- Promoting goodwill with data subjects and customers.
- Helping the organization demonstrate its compliance.

Developing, Implementing, and Maintaining an Information Security Program

Swiss laws obligate most organizations to support an information security program for one or more purposes, such as:

- To protect the personal data they collect and use (see Federal Act on Data Protection).
- To comply with applicable sector-specific guidelines (see Sector-Specific Laws and Regulations).
- To protect other forms of at-risk data, assets, and business interests (Other Laws and Regulations).

Documenting an organization's information security program may provide significant risk management benefits,

even if not explicitly required by law, for example, by:

- Demonstrating the organization's alignment with applicable industry standards (see Industry Standards).
- Prompting the organization to proactively assess risk and implement safeguards.
- Communicating information security expectations and practices to leadership, employees, customers, and other interested parties, including regulators.
- Establishing that the organization takes appropriate steps, especially if a data breach or other cyber incident occurs that may result in litigation or enforcement action.

Organizations should consider regulatory guidance and related practices when developing core program elements, including:

- **Assigning accountability.** Industry standards and regulator guidance typically call for organizations to appoint an individual responsible for information security. Swiss data protection laws foresee but do not require organizations to assign a privacy officer to oversee compliance (Article 12a, FADP Ordinance). These laws do not impose specific requirements regarding the privacy officer's location or technical qualifications.
- **Identifying and assessing risks.** Organizations must perform regular information security risk assessments to reliably identify reasonable and appropriate security measures. The Data Protection Commissioner's guidance describes four risk levels for personal data that range from low to very high risk (see Protecting Personal Data Under the FADP). FINMA Circular 2008/21 requires financial institutions to perform ongoing risk assessments that encompass all business areas, including data processing and data security.
- **Developing information security policies.** In practice, many Swiss organizations have information security policies. The Data Protection Commissioner's guidance also directs organizations to develop and maintain a data processing policy that documents the planning, development, and operation of IT resources (see Protecting Personal Data Under the FADP). Robust information security policies can help organizations by:
  - establishing information security as a core value;
  - helping employees and others to understand information security risks and take appropriate actions to minimize them; and
  - providing clear strategies and rules for using and protecting the organization's information and other IT resources.
- **Evaluating program effectiveness and compliance.** Organizations should periodically review their information security programs, especially when there is a material change in business practices, IT systems, or the risks they face. FADP Ordinance Article 8 requires organizations to periodically review the technical and organizational measures for protecting the security of personal data.

Cyber Incident Response and Data Breach Notification

A robust, well-tested incident response plan can help any organization respond more effectively to cyber incidents and data breaches (for an example plan, see Standard Document, Global Cyber Incident Response Plan (IRP)).

Swiss law does not generally mandate cyber incident response planning. However, FINMA Circular 2008/21 requires that banks develop a process for incident response. For details on responding to cyber incidents and providing data breach notification, including interacting with Switzerland's computer emergency response team (CERT) resources, see Practice Note, Cyber Incident Response and Data Breach Notification (Switzerland).

Cybersecurity Information Sharing

Switzerland supports public-private partnerships for cybersecurity information sharing through:

- The recently created Cyber Security Competence Centre and its leader, the Cyber Security Delegate, which are slated to become the overarching governmental cybersecurity contact point and competence sharing hub.
- The Reporting and Analysis Centre for Information Assurance (MELANI), which provides a forum for operators of critical national infrastructures to share cybersecurity information. MELANI will become part of the Cyber Security Competence Centre to unite the contact points.
- The Computer Emergency Response Team of the Swiss Government (GovCERT), a sub-organization under MELANI, which supports the real-time exchange of cyber threat information with other CERTs.
- The Swiss Internet Security Alliance (SISA), an independent group which lists the sharing of security information as one of its top priorities.

Switzerland is also a party to the Convention on Cybercrime of 2001, which promotes international cooperation in fighting internet fraud, child pornography, and network security violations.

Enforcement and Litigation

Regulatory Enforcement

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. For example, FINMA and OFCOM may revoke the licenses of financial services organizations and telecommunications.

Criminal provisions may also apply under the FADP, FINMASA, and the TCA.

Private Actions

Data subjects who suffer damages due to an organization's failure to implement reasonable security practices may initiate civil claims against the offenders. In practice, however, it is difficult to meet substantiality

requirements for damages claims. Swiss law does not permit class actions, so plaintiffs cannot aggregate claims to meet the substantiality requirement.

Protecting Sensitive Information Security Records

Organizations should exercise caution and protect from unnecessary disclosure sensitive information security analyses, such as risk assessments and cyber incident investigations, where possible. To trigger the attorney-client privilege, lawyers admitted to practice before Swiss courts must draft or commission the relevant documents according to a client's request. The attorney-client privilege does not apply to reports prepared for compliance or regulatory purposes.

