SWITZERLAND

Law and Practice

Contributed by:
Jürg Schneider, David Vasella and Hugh Reeves
Walder Wyss Ltd

Contents

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts and approximately 100 support staff in six offices in Switzerland's economic centres. It is an agile firm that is approachable, adapts to clients quickly, and does not hide behind formality. Because it is fully integrated, partners bring in those people who have the greatest expertise and are best suited for a particular task. This helps it avoid silos and ensures that its work is carried out by those with the greatest expertise, but also efficiently. It was the first large Swiss firm with a strong focus on tech, including data protection. Walder Wyss has one of the largest and most experienced teams in this area and advises clients in all sectors on Swiss and European data law, including privacy and related fields such as AI.

Authors

Jürg Schneider is a partner at Walder Wyss and head of the Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international issues. Jürg Schneider is a past member of the board of directors of the International Technology Law Association and past co-chair of its data protection committee. In addition, he regularly publishes and lectures on ICT topics in Switzerland and abroad.

David Vasella is a partner at Walder Wyss and co-head of the Regulated Markets, Competition, Tech and IP team. He advises Swiss and international clients on a wide range of IT and data protection matters, including compliance implementation projects, and provides clear and actionable advice on issues such as data protection, data monetisation, analytics, secrecy obligations, cloud outsourcing arrangements and advertising law. He frequently publishes and lectures in his areas of focus. He is also an editor of the Basle Commentary on the revised Swiss Data Protection and the Freedom of Information Act, and of www.datenrecht.ch, a leading information platform on data-related topics.

Hugh Reeves is a managing associate in the Regulated Markets, Competition, Tech and IP team at Walder Wyss. He advises clients on technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. He is active in the areas of data protection as well as e-commerce and assists clients with their entry or expansion into the Swiss market.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box 8034
Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

1. Basic National Regime

1.1 Laws

The Federal Constitution enshrines every person's right to privacy in their private and family life and in their home, as well as in relation to their mail and telecommunications. In addition, every person has the right to be protected against the misuse of their personal data. To anchor this protection in national law, the Federal Act on Data Protection (FADP), which had been in force since 1 July 1993, has been revised as of 1 September 2023, along with the associated Data Protection Ordinance, which regulates the details. In addition, there is another ordinance, the Federal Ordinance on Data Protection Certification (DPCO), which is relevant for data protection in Switzerland. Other laws, either sector-specific or overarching, may also apply. For example, the Swiss Civil Code protects various facets of individual personality rights. Further data protection provisions governing particular issues (eg, the processing of employee or medical data) are spread throughout several legislative acts. While the FADP governs the data processing activities of federal bodies and private individuals, data processing by the cantons or cantonal authorities is regulated on a cantonal level. Thus, in this respect, each canton has its own, additional data protection legislation.

As Switzerland is neither a member of the European Union (EU) nor of the European Economic Area (EEA), it has no general duty to implement or comply with EU laws. However, because of Switzerland's location in the centre of Europe and its close economic relations with the EU, Swiss law is in general strongly influenced by EU law, both in terms of content and interpretation. When revising the FADP, the Federal Council and Parliament took into account the international legal context, and in particular the General Data Protection Regulation of the European Union (GDPR). Owing to its extraterritorial scope, the latter has already been applied by many Swiss market actors. Despite this dependence on European Union law, the FADP is in line with Switzerland's legal tradition, as it features a high level of abstraction and is technology-neutral. It sets itself apart from the GDPR not only in its brevity, but also in the slightly different terminology it occasionally uses.

With regard to sanctions and their enforcement, the FADP deviates from the GDPR. Individuals can be punished with a criminal fine of up to CHF250,000 if they intentionally breach certain data protection provisions of the FADP. Thus, the criminal fine is not imposed on the company, but on the person responsible for the data protection violation. However, companies can also be fined up to CHF50,000 if an investigation to determine the punishable natural person within the company or organisation would entail disproportionate efforts. The offending persons are fined by the state prosecutor of a Swiss Canton, tasked with the enforcement of the FADP's criminal provisions.

The Federal Data Protection and Information Commissioner (FDPIC) – the Swiss data protection authority – does not have powers to impose criminal sanctions. However, the FDPIC enforces the administrative provisions of the revised FADP, meaning administrative measures can be taken by the FDPIC, for example by prohibiting a company from processing certain personal data in the future or by requiring it to delete specific data records (see also **2.5 Enforcement and Litigation**).

1.2 Regulators

The FDPIC is the central authority for data protection matters. The head of this supervisory

authority – the Commissioner – is elected by the United Federal Assembly (the Swiss Parliament). The term of office of the Commissioner is four years and may be renewed twice.

Under the FADP, the FDPIC has in particular the following tasks, duties and responsibilities:

- supervising federal bodies and private persons;
- advising private persons;
- assisting federal and cantonal authorities in the field of data protection,
- potentially requiring the respective business or organisation or federal body to correct, suspend, or cease certain processing of personal data, or to delete personal data (binding decisions);
- potentially requiring the respective business, organisation, or federal body concerned to comply with specific obligations, such as to inform individuals, grant a right of access, or to perform a data protection impact assessment (DPIA) (binding decisions);
- giving an opinion on draft federal legislation;
- co-operating with domestic and foreign data protection authorities;
- informing the public about the FDPIC's findings;
- approving, establishing or recognising standard data protection clauses;
- approving binding corporate rules on data protection; and
- suggesting appropriate measures to the controller, if the FDIPC has objections against the envisaged processing in the context of a possible consultation of the FDPIC regarding a DPIA.

The FDPIC may open an investigation against a federal body or a private person ex officio, or upon a data subject's complaint, if there are sufficient indications that a processing of data could violate provisions of data protection legislation.

The FDPIC has published several explanatory guidelines that increase legal certainty with respect to specific issues such as cross-border data transfers, technical and organisational measures (recently revised), DPIAs, and the processing of data in the medical sector and the processing of employee data (though these guidelines are partially outdated).

1.3 Administration and Enforcement Process

Unlike the supervisory authorities in most countries where the GDPR is enforced, the FDPIC does not have the power to impose fines on individuals, businesses or organisations.

Nevertheless, the FDPIC has the authority to impose binding administrative measures. If the federal body or the private person does not comply with the duty to co-operate, the FDPIC, may in the context of the investigation, order the following:

- access to all information, documents, registers of the processing activities and personal data which are required for the investigation;
- access to premises and facilities;
- questioning of witnesses; and
- evaluations by experts.

An addressee is entitled to appeal against the FDPIC's decisions before the Federal Administrative Court and subsequently before the Federal Supreme Court. The FDPIC may also appeal decisions of the Federal Administrative Court before the Federal Supreme Court.

1.4 Multilateral and Subnational Issues

As mentioned in **1.1 Laws**, Switzerland is neither a member of the EU nor the EEA and therefore has no obligation to implement the GDPR. Switzerland is recognised by the EU as providing an adequate level of data protection. This was decided on 26 July 2000, by the Commission of the European Communities and was confirmed on 15 January 2024.

As a member state of the Council of Europe, Switzerland has ratified the Convention ETS 108 and the Additional Protocol of 2001, and implemented them into its own law. The Convention ETS 108 is the first and, to this day, the only binding international instrument in the field of data protection law. It is part of the case law of the European Court of Human Rights (ECtHR), as it is consulted by the latter when interpreting Article 8 of the European Convention on Human Rights (ECHR). This is reflected in Swiss jurisprudence; since Switzerland has incorporated the ECHR into its own law, the ECtHR is considered the highest instance with regard to the protection of human rights. The Federal Council has also formally signed the Convention 108+ in November 2020.

Data protection laws at cantonal level only apply to data processing by the respective cantons or cantonal authorities. In addition to the revisions at the federal level, corresponding revisions of the cantonal data protection laws must also take place. To date, only a proportion have completed the necessary revision of their data protection laws; others are still in the process.

There is no agreement on mutual recognition of data protection levels between Switzerland and, for instance, the USA. Regarding the relationship between Switzerland and the UK, the UK government has the power to make its own adequacy regulations in relation to third countries such as Switzerland. At the moment, such UK adequacy regulations include Switzerland.

1.5 Major NGOs and Self-Regulatory Organisations

In Switzerland, there are self-regulatory organisations (SROs) and NGOs that are directly or indirectly committed to the protection of privacy and data protection. For example, Swico, the Swiss Association of ICT suppliers, supports its members in data protection law issues. In November 2021, for example, Swico published a charter for the ethical handling of data. All companies can voluntarily sign up to the charter, not only Swico members. The commitments in the Swico Charter are intended to contribute to a better understanding of ethical issues arising from the use of data. It is also intended to better identify ethical grey areas with regard to data protection legislation.

Furthermore, the FADP provides for the possibility for professional associations, industry associations and business associations, whose statutes entitle them to defend the economic interests of their members, as well as federal bodies, to draw up codes of conduct and submit them to the FDPIC. The FDPIC states and publishes its opinion on the codes of conduct. However, there is no obligation to submit codes of conduct to the FDPIC. In terms of content, a code of conduct can elaborate on every aspect of the FADP and thus provide assistance in its application. This could include, for example, explanations as to when a “high risk” exists or how to sufficiently anonymise in a certain industry. However, a code of conduct must be at least as strict as the FADP and must also be more specific than the FADP. The FDPIC also expects codes of conduct to include ethical considerations.

1.6 System Characteristics

In Switzerland, similarities but also differences with EU data protection law issues are perceived. Because of Switzerland's location in the centre of Europe and its close economic relations with the EU, Swiss law is in general strongly influenced by EU law, both in terms of content and interpretation (see also **1.1 Laws**). Although not identical to the GDPR, the FADP is broadly aligned with the GDPR, especially with regard to the rights of data subjects and the mechanisms in place to protect them; examples include the right to data portability and the obligation of the controller to prepare, in certain circumstances, a DPIA.

However, even if the FADP is inspired by the wording of the GDPR, Swiss law also deviates from it in some points. In most of these cases, the FADP goes less far or is less formalistic or less detailed. Only in a few cases is the FADP stricter than the GDPR. In particular, there are stricter requirements in the FADP regarding the obligation to provide information when personal data is disclosed abroad: if personal data is disclosed abroad, the data subject must be informed (eg, in the privacy policy) to which country the personal data is disclosed (though in practice, privacy notices frequently list broader regions instead of individual countries).

By comparison to EU-based authorities, Swiss authorities may often be seen as more lenient. They are, however, very active in the protection of the rights of data subjects and, with the increased powers under the revised FAPD, many expect a more "hands-on" supervisory activity.

The GDPR and the existing practice will continue to have a significant impact on the interpretation and application of the FADP. This is partly due to the fact that the GDPR has already been in effect since May 2018, and therefore more experience, legal doctrine and decisions by authorities and courts are available, even though the FADP is not a carbon-copy of the GDPR.

1.7 Key Developments

Switzerland does not have to directly implement ECJ rulings on the GDPR. However, since the FADP provides for the same adequacy mechanism and Switzerland also participated in the data protection arrangement with the USA with its own Swiss-US Privacy Shield, the Schrems II ruling was also relevant for Switzerland. The FDPIC amended the comments on the USA in its list of countries by stating that the Swiss-US Privacy Shield no longer meets the requirements for adequate data protection within the meaning of the FADP. Switzerland does not yet have a Data Privacy Framework in place, different from the GDPR, but it is expected that the Swiss version should become available by the end of March 2024.

The "new" standard contractual clauses (SCCs) published by the EU Commission on 4 June 2021, were also recognised by the FDPIC. However, in the view of the FDPIC, the new EU SCCs only allow the disclosure of personal data to states without adequate protection "provided that the necessary adaptations and additions are made for use under Swiss data protection law". From a Swiss perspective, exporters would therefore have to provide slightly supplemented SCCs (with Swiss supplements).

1.8 Significant Pending Changes, Hot Topics and Issues

One of the most important hot topics in Switzerland in connection with data protection law continues to be the revision of the Federal Data Protection Act (see **1.1 Laws** and the Swiss Trends & Developments chapter in this guide). The revised

FADP and the revised ordinances came into force on 1 September 2023, applicable immediately (except for transitional periods for some requirements). Under these circumstances, it is recommended that measures intended to make data controllers compliant with data protection law should be implemented quickly.

Additionally, it should be mentioned that the topic of SCCs remains important for Switzerland. In principle, the FDPIC recognises the new EU SCC, but has pointed out that certain modifications and additions to the EU SCCs are necessary in order to take Swiss concerns into account.

Another hot topic is AI, in particular generative AI, as well as the other upcoming data-related regulations from the EU, which may impact Switzerland-based companies as well as inspire law-makers. In relation to AI, for the time being, data protection remains the key regulation, aside from intellectual property and the protection of business secrets and obligations of professional secrecy. There are no data protection regulations specifically aimed at AI, but the general principles remain applicable, as well as requirements for contracts with providers or customers and for cross-border data transfer restrictions. There is an emerging understanding of how these issues should be tackled in relation to the use of (generative) AI, as well as an understanding of how AI governance should be addressed by companies. In relation to recent EU regulations, the Digital Services Act can apply to Swiss companies who offer services to a significant number of EEA users or target their services at an EEA audience, requiring them to adapt their terms and conditions, among other potentially applicable requirements. Moreover, the Federal Council announced in April 2023 that it is seeking to regulate large communication platforms such as Google, Facebook, YouTube and Twitter, and has mandated draft legislation for consultation by the end of March 2024.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The FADP differs in its concept from the GDPR: under the GDPR, the processing of personal data is generally prohibited unless there is a justification such as consent, the performance of contracts, legitimate interests or a statutory provision in the law. Under Swiss law, it is the other way round: data processing in the private sector is generally permitted as long as the data processing principles of the FADP are complied with, and a justification is only required in certain situations. In concrete terms, a justification is necessary if either the data processing principles are not adhered to, the data subject has objected to the processing, or particularly sensitive personal data is to be disclosed to a third party.

Personal Data

The FADP only protects the personal data and personality rights of natural persons. Data of legal entities such as commercial organisations, associations or foundations were also covered by the former FADP, which is no longer the case under the current FADP. This means that the scope of application of the revised legislation coincides with that of the GDPR. Personal data entails all information that can be linked to a natural person (for instance name, address or nationality).

Data Processing Principles

Personal data may only be processed lawfully; ie, not in violation of another norm of Swiss law

which directly or indirectly aims to protect the personality.

The processing must be proportionate. Proportionate means that data processing may only go as far as it is necessary, appropriate and proportionate in the narrow sense for the purpose pursued.

Personal data must then be processed in good faith. This means that the processing shall be apparent to the data subject.

Personal data may only be processed for the purpose that was stated when it was obtained, that is evident from the circumstances or that is provided for by law. If the purpose of the processing changes, the consent of the data subjects must be obtained or there must be other overriding interests.

Accuracy of data is also important. This means that the data must be up-to-date and that it must be possible to correct incorrect data.

The amended FADP stipulates that the data must be destroyed or made anonymous as soon as it is no longer required for the purpose of processing. Fulfilment of this obligation requires that the controller determines retention periods in advance.

Personal data may not be processed against the explicit will of the data subject. This is a particularly central principle in Swiss data protection law, because unlike under the GDPR, the FADP does not require a legal basis for the processing of personal data, but relies on an "opt-out" principle: if the data subject does not want data to be processed, they must object to the processing. It is not necessary to give a reason for objecting. Conversely, this means that if a private person (ie, not a public authority) wants to process personal data for a specific purpose and complies with the processing principles, it is allowed to do so provided the data subject does not object. Consent is not per se required, not even in the case of particularly sensitive personal data, although the FDPIC has sometimes argued the opposite.

Justification for a Breach of Privacy

If a private entity breaches one or several of the processing principles, this constitutes a violation of the data subject's personality rights. Such a breach of personality rights is unlawful unless it is justified by the consent of the injured party, by an overriding private or Swiss public interest or by Swiss law.

This system of justification does not apply to federal bodies; instead federal bodies may process personal data only if there is a statutory basis for doing so.

Profiling With and Without "High Risk"

"Profiling" is any type of automated processing of personal data which seeks to evaluate certain personal aspects relating to a natural person. In particular it attempts to analyse or predict aspects of that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or change of location. In addition, there is also "high-risk profiling". This is a profiling that entails a high risk to the personality or fundamental rights of the data subject by leading to a combination of data that allows an assessment of essential aspects of the personality of a natural person.

Automated Individual Decision-Making

The controller must inform the data subject of a decision which is based exclusively on auto-

mated processing and which entails a legal consequence for the data subject or significantly affects that person. The data subject may request that the automated individual decision be reviewed by a natural person.

Privacy by Design and by Default

The FADP enshrines the principles of privacy by design (data protection through technology design) and privacy by default (only data that is absolutely necessary to a specific purpose is processed, and this should be set out before data processing starts). These principles require authorities and businesses to implement the processing principles of the FADP from the planning stage by putting in place appropriate technical and organisational measures.

Data Protection Impact Assessment

Similarly to the GDPR, the data controller under the FADP must prepare a DPIA prior to data processing if the data processing may entail a high risk to the personality or fundamental rights of the data subject. A high risk arises, in particular where new technologies are used, from the type, scope, circumstances and purpose of the processing (ie, in the case of extensive processing of sensitive personal data and when extensive public areas are systematically monitored).

The content of a DPIA includes the measures for the protection of personality and fundamental rights. If the DPIA shows that the planned processing will still result in a high risk to the personality or fundamental rights of the data subject despite the measures that the controller envisages, the controller shall obtain the FDPIC's opinion in advance.

Inventory of Processing Activities

The FADP requires that data controllers and processors keep an inventory. This inventory is intended to record the various processing activities of a company and provide the controller and the processor with an overview of the data protection-relevant activities in the company. If the FDPIC investigates a case in the future, the first thing the Commissioner will probably ask for is the inventory of processing activities. The inventory contains the essential data protection parameters of the various data processing operations, but no personal data itself. The minimum content of the directory is specified in the law, in particular the identity of the controller, the purpose of the processing, the description of the categories of personal data and the persons concerned (eg, customers, employees), the categories of data recipients (eg, group companies, service providers, authorities, media, the public), the retention period, etc. There are no formal requirements for the inventory of processing activities; an Excel sheet is just as sufficient as a sophisticated IT solution. However, the Data Protection Ordinance provides for exceptions from the obligation to keep an inventory of processing activities. In principle, an inventory does not have to be kept if a company has fewer than 250 employees (per headcount, not FTE, and part-time employees, trainees etc, also count as employees). In addition, there are counter-exceptions in the Data Protection Ordinance, meaning a company must still keep an inventory even though it has fewer than 250 employees if either:

- a company carries out extensive processing of particularly sensitive personal data. This includes, for example, organisations and companies whose very purpose entails the processing of particularly sensitive personal data; or
- a high-risk profiling is carried out, meaning if a profiling entails a high risk for the personality or the fundamental rights of the data sub-

ject by combining data that allows an assessment of essential aspects of the personality of a natural person; eg, with regard to statements about financial circumstances, family circumstances, educational background, political views.

An inventory of processing activities can help with data protection compliance and it can therefore make sense to keep a processing directory even if a company is not legally obliged to do so. Certain companies contractually stipulate that the contracting party must keep an inventory, meaning that, for example, a controller requests that its processor must keep an inventory.

Data Protection Adviser

The FADP has the role of a data protection adviser (DPA), which is a similar function as a DPO under the GDPR. However, unlike under the GDPR, the designation of a DPA for private businesses is always optional; it is only mandatory for federal bodies.

The DPA is the contact point for the data subjects and for the competent data protection authorities responsible for data protection matters in Switzerland. A DPA may, but does not have to, be an employee of the business.

The advantages of appointing a DPA are mainly related to reputation and proper corporate governance. In addition, if a DPIA shows that the data processing poses a "high risk" to the data subjects despite mitigating measures, the controller must consult the FDPIC prior to the processing. However, a private controller could abstain from approaching the FDPIC if it consulted the DPA instead. The function of the DPA is tied to certain requirements in this regard: The adviser performs their function towards the controller in a professionally independent manner and without being bound by instructions; the adviser does not perform any activities which are incompatible with their tasks as DPA; they possess the necessary professional knowledge; the controller publishes the contact details of the DPA and communicates them to the FDPIC.

Privacy Notice

By comparison to the GDPR, the FADP places less of an onus on (internal and external) documentation. That said, however, the revised FADP does state that the controller shall inform the data subject appropriately about the collection of personal data. There is no formal requirement for the fulfilment of this duty. In practice, it usually takes the form of a privacy notice.

In this context, it is sufficient under Swiss law if the data controller informs the data subject where they can obtain the privacy notice, provided the controller can reasonably expect the data subject to retrieve or view this document.

Notification of Data Security Breaches

The controller must notify the FDPIC of any data security breach that is likely to result in a high risk for the data subjects. The notification must be made as soon as possible (which is maybe shorter than the 72-hour maximum time provided for in the GDPR, but potentially also longer). The threshold for the notification obligation is higher than under the GDPR. In addition, where necessary for the protection of the data subjects or on instruction by the FDPIC, the controller must inform the data subjects of the breach.

Logging Obligations

A private controller or processor must at least log the storage, modification, reading, disclosure, deletion and destruction of the data (including identity of the person who carried out the processing, type, date and time of processing), if

sensitive personal data is processed automatically on a broad scale or if a high-risk profiling is carried out and preventive measures cannot guarantee data protection. Data must be stored for at least one year, separately from the system in which the data is processed. However, there are likely no criminal sanctions for non-compliance, as this should not be seen as a matter of security.

2.2 Sectoral and Special Issues

Sensitive Personal Data

Certain categories of data are subject to special protection in the revised FADP due to their intrinsic sensitivity and thus the increased risk potential of their processing for the privacy of the data subjects.

These special categories of personal data relate to:

- religious, ideological, political or trade union-related views or activities;
- health, intimate sphere or racial or ethnic origin;
- genetic data;
- biometric data which uniquely identifies a natural person;
- data on administrative and criminal proceedings or sanctions; and
- data on social security measures.

For sensitive personal data, more stringent requirements apply, in particular to the consent of the data subjects to their processing (if consent if required). If extensive processing of particularly sensitive personal data is planned, there may be a high risk that leads to private data controllers having to carry out a DPIA in advance.

Data Subject's Rights

Data subjects have the right to object to data processing. Provided that the processing meets the applicable conditions and no legal exceptions apply, data subjects then have the right to:

- request information about the personal data stored;
- have incorrect or incomplete personal data corrected;
- object to further processing and request the deletion or anonymisation of the data subject's personal data, forcing the controller to justify any continued processing;
- receive certain personal data in a structured, commonly used and machine-readable format; and
- withdraw consent with effect for the future, if processing is based on consent.

Cookies

Since 2007, the use of cookies has been regulated in the Swiss Telecommunications Act. Website operators must inform the user about the processing and its purpose, but it is not mandatory to use a cookie banner under Swiss law. They must also note that the user may refuse to allow processing and how cookies can be deactivated in the user's browser. In Switzerland, the opt-out principle applies. If a cookie banner is used then, depending on how it works, the principle of privacy by default may apply.

Financial and Health Data

In addition to the FADP, many sectors are governed by special laws that also contain data protection provisions. For instance, when dealing with personal data of bank customers, so-called "Client Identifying Data" (CID), in the financial and banking sector, in addition to the data protection principles of the FADP, banking secrecy under the Banking Act applies. In light

of this, the Swiss Financial Market Supervisory Authority (FINMA) has defined certain technical and organisational requirements regarding the handling of critical data for banks and securities dealers (Circular 2023/1 Operational risks and resilience). This circular imposes a notification duty in certain cases of data breaches and sets out additional governance and risk-management obligations. Where significant functions are outsourced, the Circular 2018/3 Outsourcing places additional obligations on banks and insurance companies, including for the agreement with the provider.

Data about health is still considered to be "sensitive personal data" under the revised FADP. The revised FADP also explicitly includes "genetic data" and "biometric data". The processing of such data in a specific individual case must not only be in accordance with the FADP, but also with the Human Research Act and the Federal Act on Human Genetic Testing. This corresponding co-ordination of the laws is not always trivial, especially with regard to the duty to provide information and the consent requirements, which are of particular importance in the area of health data.

2.3 Online Marketing

The admissibility of advertising is regulated by the Federal Act of Unfair Competition (UCA). It imposes certain limitations on electronic mass advertising. The sender may only contact target customers via electronic mass advertising if it cumulatively:

- obtains the target customer's affirmative consent (opt-in-system) in advance (in this context it is recommended that the customer consents in text form for example through the activation of a tick-box upon completion of an online form);
- provides the sender's correct and complete contact information; and
- displays a reference to an easy option to refuse future marketing materials – this reference must be evident and clearly visible each time the sender contacts the customer and the customer must have the possibility to promptly refuse to receive any further marketing materials on the same channel of communication, with no extra effort and costs.

Mass advertising may reach existing customers without their prior consent, if cumulatively:

- the sender obtained the customer's contact information at the occasion of the purchase of a product or service;
- the sender had informed the customer, when obtaining their personal information, about the possibility to opt-out from direct marketing;
- the direct marketing refers to own and similar products, services or works, for which the customer has shown interest – marketing for other (own) products/services from the sender or third-party products/services is not permitted (similarity is given where the purchased product or service is interchangeable);
- the sender provides its correct and complete contact information; and
- the sender provides a reference to an easy, free-of-charge option to refuse future marketing materials.

Another option for the accomplishment of the marketing campaign could be the use of postal mail. As printed marketing is not in scope of Article 3 (1) of the UCA, postal mass advertising is generally permitted. Data protection restrictions may, however, apply where individuals have

expressly objected to the use of their address for marketing purposes.

Non-compliance with anti-spam legislation may result in a civil law claim by individuals, consumer protection organisations or (under certain limited conditions) the federal government. Further, deliberate non-observance of the dedicated provision of the UCA constitutes a criminal offence. It should be noted, however, that enforcement of anti-spam legislation is not particularly rigorous in Switzerland.

2.4 Workplace Privacy

The FADP covers the processing of data on employees by employers. The Swiss Code of Obligations (SCO) also contains specific provisions on data processing and the protection of the privacy of employees.

Most importantly, the employer must – within the employment relationship – acknowledge and safeguard the employee's personality rights, have due regard for their health and ensure that proper moral standards are maintained. The employer must refrain from any interference with the personality of the employee that is not justified by the employment contract and, within the framework of the employment relationship, prevent any such interference by superiors, employees or third parties. Excessive employee surveillance, for example, may be unlawful under public labour regulations.

These provisions of the SCO and the FADP are closely intertwined and the employer may only process data on employees in two cases and only to a rather limited extent.

- Before the conclusion of an employment contract and during its implementation, data on job applicants may be processed in order to clarify whether they are suitable for the job in question.
- During the employment period, data on employees may be processed that is necessary for the performance of the employment relationship.

However, recent Swiss Supreme Court case law adds some flexibility and leaves some room for employer private interest justifications. This approach is comparable to the GDPR in the sense that an overriding private interest could justify the processing of employee data that the employment law and the SCO would otherwise not cover.

Whistle-Blowing

Since 2008, a partial revision of the SCO (protection in case of reporting irregularities at the workplace) has been discussed in parliament. The Federal Council wanted to create clear legal rules on when whistle-blowing is lawful. In March 2020, the Federal Council's bill on the protection of reports of irregularities in the workplace was definitively rejected for the second time since 2015. Therefore, there will be no legal reform of whistle-blowing in Switzerland in the near future.

In Switzerland, unlike in the EU, there are no mandatory whistle-blowing hotlines, and the use of whistle-blowing hotlines is not specifically regulated by the FDPA or the CO. However, from a FDPA and CO perspective, whistle-blowing hotlines can be used if certain minimum requirements are met, such as:

- the transparent informing (especially of employees and contractors) of the existence of the whistle-blowing hotline;
- the informing of relevant employees, contractors, etc, of allegations about them contained in a specific whistle-blowing report, unless

there is an overriding interest not to do so in order to protect the ensuing investigations or the reporting person;
- adequate safeguards to protect the data subjects from false or slanderous accusations; and
- strong state-of-the-art security measures.

This being said, it is important to verify compliance on an individual basis before implementing a whistle-blowing hotline.

2.5 Enforcement and Litigation

The FDPIC

The FDPIC must carry out ordinary administrative procedures under the FADP and issue corresponding rulings if it wants to intervene. Unlike its EU counterparts, however, the FDPIC may not fine offending data controllers and commissioned processors – this competence is the responsibility of the cantonal criminal prosecution authorities (see **1.1 Laws** and **1.3 Administration and Enforcement Process**).

The FDPIC must prosecute breaches of the data protection provisions of the FADP ex officio. Anyone can report such violations to the FDPIC; a report in the press can also be sufficient. However, the FDPIC can refrain from opening an investigation in the case of violations of "minor importance". Also, wherever the FDPIC is of the opinion that appropriate "recommendations" are sufficient to restore the lawful state of affairs, they will probably be able to invoke the possibility of waiving the opening of an investigation. In such cases, the FDPIC can terminate formal proceedings prematurely by issuing a "warning". This is likely to become the standard and help to keep the burden low for all parties involved. In addition, the FDPIC only has to initiate proceedings if there are "sufficient indications" of a data protection breach.

The FDPIC's information gathering plays out in two stages.

- At the first stage, information is obtained by simple request; the requested private persons or federal bodies are in principle obliged to co-operate and must provide the FDPIC with all documents that are necessary for the investigation.
- If this is insufficient, the FDPIC has the power to obtain the information and insight necessary for the investigation by means of compulsory measures (if necessary, with the help of other federal authorities and cantonal or communal police bodies).

If the FDPIC has established a violation of the data protection provisions of the FADP, it is authorised to issue a corresponding ruling – an administrative measure. In doing so, the FDPIC may demand the modification, interruption or termination of a data processing operation, the erasure of the processed personal data and the implementation of the accompanying measures and the rights of the data subjects.

The addressee of the ruling may appeal against the FDPIC's ruling to the Federal Administrative Court and refer its decision to the Federal Supreme Court; the FDPIC may also lodge an appeal against appeal decisions issued by the Federal Administrative Court.

Penalty Provisions

The criminal fine framework in the FADP has a limit of CHF250,000. For instance, private persons are liable to a criminal fine of up to CHF250,000 if they wilfully provide false information to the FDPIC in the context of an investigation or wilfully refuse to co-operate.

The cantons are responsible for the prosecution and the judgment of criminal acts (see also **1.1 Laws**). The fines are directed against the responsible natural person, unlike in the GDPR, where the fines are directed against the respective company and where the fines do not have a criminal character. The widespread view is that, given the criminal law nature of the Swiss fines, they are neither insurable nor may the company pay them for the natural person. These circumstances – especially the criminal character of the fine – makes the penalty provisions in the FADP in principle more "punitive" compared to the GDPR. However, in Switzerland, only the intentional breach of the FADP is punishable, and the catalogue of offences is smaller than that of the GDPR. It was the legislature's assumption that the fines will create psychological pressure in companies – especially among management – to comply with data protection laws, and experience shows that data protection indeed has increased boardroom attention.

Private Litigation

The data subject can, in a civil lawsuit, claim damages and the handing over of profits, as well as concrete measures concerning the data processing (for instance a total or partial ban on the data processing in question). The revision of the FADP introduced changes to civil procedure law that facilitates private enforcement to an extent.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

In Switzerland, there are fundamental rights that must be respected if authorities wish to access data. According to the Federal Constitution, every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications (see **1.1 Laws**).

Criminal prosecution authorities have the right to obtain information by means of provisions in the Swiss Criminal Procedure Code (CrimPC). In order to secure evidence (and thereby obtain data), among other things, the criminal prosecution authorities have at their disposal a set of compulsory measures under the CrimPC.

In particular, secret surveillance measures (eg, surveillance of postal and telecommunications traffic or surveillance with special technical devices for the surveillance of telecommunications) see regular use.

Depending on the type of compulsory measure, the competence lies with the police, the public prosecutor's office (in principle responsible for ordering compulsory measures, but in the field of secret compulsory measures it needs the approval of a court for compulsory measures) or the court. In principle, compulsory measures can be challenged by means of an appeal, though such challenges may, depending on the situation, only occur once the measures have taken place.

3.2 Laws and Standards for Access to Data for National Security Purposes

Whether and under what conditions the authorities can access the data depends on the specific facts of the case and the investigating authority. The most extensive access to data is granted to law enforcement authorities (see **3.1 Laws and Standards for Access to Data for Serious Crimes**) and the intelligence service.

According to the Federal Act on the Intelligence Service (IntelSA), the Federal Intelligence Service

can, if necessary, access data collected by other federal or cantonal authorities. This also applies to data from law prosecution authorities, in particular data originating from the surveillance of postal and telecommunications traffic pursuant to the Federal Act on the Surveillance of Post and Telecommunications (SPTA). According to the SPTA, Swiss telecoms providers are generally obliged to store the metadata of their users and to hand it over to criminal investigators in case of founded suspicions. For this purpose, the companies must store, for at least six months, data pertaining, for instance, to phone numbers dialled, call duration and so forth. The law attempts to strike a balance between the interests of private individuals in protecting their privacy and the law enforcement interests of the state.

The IntelSA focuses on preventive surveillance by the federal intelligence service in various forms and without concrete suspicion of a criminal offence. The SPTA, on the other hand, serves to enable law enforcement authorities to access certain communication and envelop data of postal and telecommunications traffic within the framework of specific criminal proceedings.

3.3 Invoking Foreign Government Obligations

Blocking statutes limit the sharing of personal data abroad with foreign authorities. Accordingly, organisations typically cannot invoke foreign government access requests as a lawful basis for a direct cross-border transfer of personal data (and its prior collection). Rather, such requests must go through the channels of international legal assistance.

Switzerland has concluded a mutual legal assistance treaty in criminal matters with the USA. However, Switzerland has not concluded a CLOUD Act Executive Agreement with the USA.

As a side note, in order to be able to exchange personal data with the EU and its member states without restriction, Switzerland must continue to be recognised by the European Commission as a third country with an adequate level of data protection pursuant to Article 45 of the GDPR, and Switzerland's adequacy was indeed confirmed on 15 January 2024.

3.4 Key Privacy Issues, Conflicts and Public Debates

One of the most discussed topics in the field of data protection in Switzerland has, for almost ten years, been data retention in the field of telecoms surveillance. In particular, telecommunications and internet service providers must retain records of their customers' communications data on behalf of the state; eg, who called whom and for how long, who logged on to the internet and for how long, who sent an email or text message to whom and when, and the location information of the mobile phone. The service provider must retain such data for six months and release it to law enforcement agencies or the intelligence service upon request. In other words, data is retained without suspicion of a crime. However, the police and the prosecution authorities do not have unlimited access to the data, as it remains in the possession of the telecommunications services provider, not of the state. The law also sets in place high barriers to access (see **3.1 Laws and Standards for Access to Data for Serious Crimes**) – access is only possible if several preconditions are met. Previous investigations must have been unsuccessful or the enquiries would otherwise have little prospect of success or would be made disproportionately more complex.

Another key topic is cross-border transfers. Switzerland follows the Schrems-II approach and requires a transfer impact assessment prior to a transfer abroad on the basis of the standard contractual clauses (see **4.2 Mechanisms or Derogations That Apply to International Data Transfers**). Because Switzerland does not yet have a Swiss-US Data Privacy Framework, this applies to transfers to all US recipients (unless these are based on an exemption).

Related to cross-border transfers, the use of cloud services is largely accepted, including for regulated industries and market participants operating under obligations of professional secrecy. However, the finer details remain a matter of debate, in particular for banks and other regulated financial market participants, as well as for federal and cantonal authorities.

Data subject rights continue to be debated as well, particularly access requests. There is established case law that access requests made solely in order to collect evidence in view of claims are abusive and can rejected, but the details remain open. In view of the broader access right under the revised FADP, it can be expected that subject right requests will grow in number and will raise additional questions.

Finally, the rise of generative AI raises privacy-related questions, along with issues of intellectual property law and the protection of business or professional secrets. There is no AI regulation in Switzerland at this time, aside from light regulation for federal bodies, but it is expected that the federal government will propose approaches to regulation by the end of 2024. This will likely address privacy-related issues, among others.

4. International Considerations

4.1 Restrictions on International Data Issues

The FADP aims to protect the personality rights and the fundamental rights of natural persons whose personal data is processed. As a consequence, the FADP contains provisions on how this protection is to be guaranteed when data is transferred abroad, for instance, to a state that does not offer the same level of data protection as Switzerland does.

Controllers or processors may transfer personal data abroad if the Federal Council has determined that the legislation of the relevant state or international body guarantees an adequate level of protection. Therefore, the Federal Council determines, in a binding manner, to which countries the export of data is permitted.

On the other hand, in the absence of such a decision by the Federal Council, personal data may be disclosed abroad only if appropriate protection is guaranteed. Thus, at least one of the following conditions must be fulfilled:

- an international treaty;
- data protection provisions of a contract between the controller or the processor and its contracting partner, which were communicated beforehand to the FDPIC;
- specific safeguards prepared by the competent federal body and communicated beforehand to the FDPIC;
- standard data protection clauses previously approved, established or recognised by the FDPIC; and
- binding corporate rules on data protection which were previously approved by the FDPIC, or by a foreign authority which is responsible for data protection and belongs

to a state which guarantees adequate protection.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

The FADP provides that personal data may not be disclosed abroad if this would seriously endanger the personality of the persons concerned. Such a serious threat to the personality rights of the data subject may arise if the exporting state does not have legislation that guarantees an adequate level of data protection. However, a transfer of data to such a state may be permitted if one of the conditions described in **4.1 Restrictions on International Data Issues** is fulfilled.

Regarding SCCs (see also **1.7 Key Developments** and **1.8 Significant Pending Changes, Hot Topics and Issues**) the FDPIC formally recognised the new SCCs, which the European Commission had adopted on 4 June 2021, for international transfers from Switzerland to third states, but only if adaptations are made which are necessary under Swiss data protection law. By recognising the new SCCs, the FDPIC reduces uncertainties in a post-Schrems II era and helps companies ensure the ongoing lawful transfer of personal data.

Due to the extraterritorial reach of the GDPR, some data transfers may additionally be subject to the GDPR, in particular if data pertaining to EU residents is (also) transferred. Therefore, two cases should be distinguished:

- in the first case, there is no link to the GDPR, and the data transfer is subject solely to the FADP; and
- in the second case, the GDPR applies to certain data transfers based on its extraterritorial reach, but the data exporter is a controller or a processor that falls within the scope of the FADP (eg, because it is located in Switzerland).

For data transfers subject to the GDPR, the non-amended SCCs will be applicable. Therefore, the parties must determine whether only the FADP or both the FADP and the GDPR apply to their specific circumstances. In the second case, the GDPR applies to certain data transfers based on its extraterritorial reach, but the data exporter is a controller or a processor that falls within the scope of the FADP; eg, because it is located in Switzerland. On the other hand, SCCs for data transfers subject to the GDPR may not be amended. Therefore, the parties must determine whether only the FADP or both the FADP and the GDPR apply to their specific circumstances.

The new EU SCCs require the implementation of a "transfer impact assessment" (TIA). This also applies to Swiss companies if they use the new EU SCCs. As part of a TIA, the Swiss data exporter must check in each specific case whether the laws of the recipient country regarding official access in the recipient country (eg, for the purpose of national security or criminal prosecution) and the rights of the data subjects are compatible with Swiss data protection law and Swiss constitutional principles. According to the FDPIC, the Swiss data exporter must carry out the corresponding clarifications itself and must not rely solely on the statements of the data importer.

Switzerland does not yet have a Swiss-US Data Privacy Framework (DPF) in place, but it is expected that the Swiss version of the DPF will be available by the end of March 2024.

Finally, the FDPIC has pointed out that internal company data protection regulations, so-called binding corporate rules (BCR), cannot be a sub-

stitute for the conclusion of SCCs, if transfers are made outside of a group of companies subject to the BCRs.

4.3 Government Notifications and Approvals

Personal data may be disclosed abroad if the Federal Council has determined that the legislation of the relevant state or international body guarantees an adequate level of protection. In this case, an approval by the FDPIC is not required.

In the absence of an adequacy decision by the Federal Council, personal data may be disclosed abroad only if appropriate protection is guaranteed by certain conditions (see **4.1 Restrictions on International Data Issues**). Also in this case, no explicit notification or approval is required for the specific data transfer, but some conditions may apply. For instance, SCCs must have been previously approved, established or recognised by the FDPIC.

By way of derogation to the above (meaning even if it exists no adequacy decision and no appropriate protection is guaranteed), in certain cases personal data may nevertheless be disclosed abroad, though the controller or processor must inform the FDPIC of this disclosure, but only upon request. These are the following cases:

- the disclosure is directly connected with the conclusion or the performance of a contract between the controller and its contracting partner in the interest of the data subject;
- the disclosure is necessary in order to safeguard an overriding public interest, or for the establishment, exercise or enforcement of legal claims before a court or another competent foreign authority;
- the disclosure is necessary to protect the life or the physical integrity of the data subject or a third party and it is not possible to obtain the consent of the data subject within a reasonable period of time; and
- adequacy decision – the countries which are considered by the Federal Council to have an adequate level of data protection can be found in the list in Annex 1 of the Data Protection Ordinance.

4.4 Data Localisation Requirements

There are no specific data localisation requirements under Swiss data protection law. However, some exceptions may apply to regulated activities. For example, the Ordinance on the Electronic Patient Dossier explicitly states that the data repositories (of health data) must be located in Switzerland and must be subject to Swiss law. In addition, various provisions require that certain data remain accessible at all times from Switzerland, such as some client data processed by banks and insurance companies, but this does not usually prevent cross-border transfers or storage abroad of that data.

4.5 Sharing Technical Details

There are no obligations under Swiss law to share software code, algorithms or similar technical details with the government. It can be noted however that in certain cases of telecommunications surveillance, the service provider may be asked to remove encryption over data in its possession.

4.6 Limitations and Considerations

In the event of data requests from foreign authorities, foreign litigation proceedings, or internal investigations, the general provisions for international data transfers (see **4.2 Mechanisms or Derogations that Apply to International Data Transfers**) and for requests from foreign authori-

ties (see **3.3 Invoking Foreign Government Obligations**) apply.

Blocking statutes may apply as well (see **4.7 "Blocking" Statutes**).

4.7 "Blocking" Statutes

Swiss law contains so-called blocking statutes that can prevent or hinder the collection of evidence in multi-jurisdictional proceedings. As soon as an internal investigation is carried out at the request of a foreign authority or the results of such an investigation are generated with the aim of making them available to a foreign authority, two provisions of the Swiss Criminal Code (SCC) must be taken into account: Article 271 of the SCC (unlawful activities on behalf of a foreign state) and Article 273 of the SCC (industrial espionage).

According to Article 271 of the SCC, anyone is liable to punishment, who carries out activities on behalf of a foreign state, a foreign party or foreign organisation, on Swiss territory without lawful authority, where such activities are the responsibility of a public authority or public official, or who facilitates such activities. The taking of evidence constitutes a sovereign judicial function of the courts rather than of the parties. Therefore, the taking of evidence for a foreign state court or for foreign regulatory proceedings constitutes an act of a foreign state. If such acts take place in Switzerland, they violate Swiss sovereignty and are prohibited under Article 271 of the SCC, unless they are authorised by the competent Swiss authorities or take place within the framework of mutual legal assistance proceedings. A violation of Article 271 of the SCC is punishable by imprisonment of up to three years or a fine of up to CHF540,000, or both. It is important to be aware that the transmission of evidence abroad to comply with a foreign order requiring the production of evidence does not prevent the application of Article 271 of the SCC. Furthermore, evidence can only be handed over to foreign authorities lawfully by following mutual legal assistance proceedings or by obtaining authorisation from the competent Swiss authorities.

The blocking statute in Article 273 of the SCC additionally prohibits industrial espionage. According to this article, anyone who seeks to obtain a manufacturing or trade secret in order to make it available to an external official agency, a foreign organisation, a private enterprise, or the agents of any of these; or anyone who makes a manufacturing or trade secret available to a foreign official agency, a foreign organisation, a private enterprise, or the agents of any of these is criminally liable.

Therefore, manufacturing and business secrets with sufficient connection to Switzerland may only be released or communicated abroad when:

- the owner of the secret relinquishes its intent to keep the information secret;
- the owner of the secret agrees to disclose this information;
- all third parties (who have a justifiable interest in keeping the information secret) consent to such a disclosure;
- Switzerland has no immediate sovereign interest in keeping the information secret; and
- all requirements set forth by the DPA (in particular, as regards cross-border transfers) are complied with.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

In Switzerland, the topics of AI and the internet of things (IoT), etc, are being discussed in particular at an academic level. At a political level, the Federal Council started a "Digital Switzerland Strategy" in 2018. In this context, an interdepartmental working group (especially regarding AI) was set up. In December 2019 the group published a report in which it explained the challenges regarding AI for Switzerland. The report states that relevant legal principles in Switzerland are usually formulated in a technology-neutral way so that they could also be applied to AI systems. Therefore, the existing legal framework would already permit and limit the use of AI in principle (eg, the Federal Act on Gender Equality), and also applies in particular to discrimination that may arise as a result of AI decisions. Thus, according to this report, there would be no need for fundamental adjustments to the existing legal framework. In 2020, the same interdepartmental working group then developed guidelines on the use of AI within the Federal Administration, meaning a general frame of reference for federal agencies and external partners entrusted with governmental tasks. The guidelines were adopted by the Federal Council in November 2020.

However, current developments at the European Union level (for instance the forthcoming Artificial Intelligence Act) have an impact on Switzerland. Switzerland, given its economic and geographical position vis-à-vis the EU, will also have to deal with many of these topics, especially because many of the planned EU laws also have extraterritorial effects and thus also apply to Swiss actors. The Swiss Federal Council has therefore instructed the Federal Department of the Environment, Transport, Energy and Communications to prepare an overview of potential regulatory approaches to AI, which is expected to be available by the end of 2024. Until then, data protection law, intellectual property law and laws protecting secret information continue to be the key framework for dealing with AI.

5.2 "Digital Governance" or Fair Data Practice Review Boards

In Switzerland there are no requirements to have digital governance boards or a data ethics commission. However, the topic of data ethics is becoming increasingly important, especially for companies since the end of 2021 (see **1.5 Major NGOs and Self-Regulatory Organisations**). Also, large and multinational companies active in Switzerland foresee such review boards and committees.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

Please refer to **2.5 Enforcement and Litigation**.

5.4 Due Diligence

Over the past ten years, data protection has gained more and more importance in the context of M&A transactions. Checking the target company's compliance with data protection laws has certainly become an essential part of any due diligence (DD) process.

It is of particular relevance to check whether the target itself is compliant with data protection law, and to what extent (in case of any compliance shortcomings). For instance, it must be ascertained whether the target company has systematically integrated data protection into its processes and whether responsibilities for compliance with the legal requirements are clearly allocated.

Moreover, the DD process should identify any data protection liabilities, either arising from data subject or third-party claims, or from gaps in the data protection documentation or practices.

5.5 Public Disclosure

There are currently no laws requiring the disclosure of an organisation's risk profile or cybersecurity experience.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

Switzerland does not specifically consider new laws, projects or strategies like those of the EU, with the exception of the Digital Markets Act and the Digital Services Act. Two motions calling for the implementation of the objectives of the Digital Services Act and the Digital Markets Act were submitted to the National Council in March 2023, and are pending in Parliament. In addition, the Federal Council instructed the Federal Office of Communications, at the beginning of April 2023, to prepare a consultation draft on the regulation of online platforms by March 2024. In addition, Switzerland is closely observing and discussing current developments in the EU, including the AI Act (see **5.1 Addressing Current Issues in Law**).

5.7 Other Significant Issues

Another major topic is the issue of cyber-attacks in Switzerland. In recent years, the number of cyber-attacks on the infrastructure of Swiss companies in Switzerland increased significantly. This worrisome trend has also shown the relative exposure of many Swiss companies, of all sizes, as well as public bodies, and is an alarming reminder of the ubiquity and damaging nature of cyberthreats.

In December 2022, the Federal Council submitted a draft bill to Swiss Parliament to amend the Federal Information Security Act. This draft creates the legal basis for the obligation of operators of critical infrastructures to report cyber-attacks they have been subjected to. The term "critical infrastructure" does not only include energy supply companies, hospitals, civil aviation, or telecommunications providers – universities, authorities at all federal levels, banks, insurance companies and financial market infrastructure may also fall within the scope. It is expected that the revised regulation will enter into force by 1 January 2025.

Trends and Developments

Contributed by:
Jürg Schneider, David Vasella and Hugh Reeves
Walder Wyss Ltd

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts and approximately 100 support staff in six offices in Switzerland's economic centres. It is an agile firm that is approachable, adapts to clients quickly, and does not hide behind formality. Because it is fully integrated, partners bring in those people who have the greatest expertise and are best suited for a particular task. This helps it avoid silos and ensures that its work is carried out by those with the greatest expertise, but also efficiently. It was the first large Swiss firm with a strong focus on tech, including data protection. Walder Wyss has one of the largest and most experienced teams in this area and advises clients in all sectors on Swiss and European data law, including privacy and related fields such as AI.

Authors

Jürg Schneider is a partner at Walder Wyss and head of the Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international issues. Jürg Schneider is a past member of the board of directors of the International Technology Law Association and past co-chair of its data protection committee. In addition, he regularly publishes and lectures on ICT topics in Switzerland and abroad.

David Vasella is a partner at Walder Wyss and co-head of the Regulated Markets, Competition, Tech and IP team. He advises Swiss and international clients on a wide range of IT and data protection matters, including compliance implementation projects, and provides clear and actionable advice on issues such as data protection, data monetisation, analytics, secrecy obligations, cloud outsourcing arrangements and advertising law. He frequently publishes and lectures in his areas of focus. He is also an editor of the Basle Commentary on the revised Swiss Data Protection and the Freedom of Information Act, and of www.datenrecht.ch, a leading information platform on data-related topics.

Hugh Reeves is a managing associate in the Regulated Markets, Competition, Tech and IP team at Walder Wyss. He advises clients on technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. He is active in the areas of data protection as well as e-commerce and assists clients with their entry or expansion into the Swiss market.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box 8034
Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

Introduction

Three key topics currently in the Swiss data protection and privacy space are: the entry into force of the revised Swiss Data Protection Act (FADP) on 1 September 2023, the renewal of the EU Commission's adequacy decision for Switzerland and the future introduction of an obligation to report cyber-attacks on critical infrastructures.

The entry into force on 1 September 2023 of the revision of the FADP, in particular, is a crucial development for companies in Switzerland. Businesses that have not yet done so should finalise their assessment of their compliance with the revised FADP and, if necessary, implement all actions and measures to meet the requirements of the revised FADP.

Hot Topic One: The Revised Federal Act on Data Protection (FADP)

The advent of the European Union's new General Data Protection Regulation (GDPR), which became effective in 2018, has put additional pressure on the Swiss legislature. The GDPR applies to the entire European Economic Area (EEA) and has a potentially worldwide reach due to its extraterritorial scope. Many Swiss companies fall within the scope of the GDPR as well due to their orientation towards the EEA.

The revised FADP entered into force on 1 September 2023. It largely follows the GDPR's approach. However, the FADP is less formalistic and has less specific regulatory content. There are only a few points where the new FADP is stricter than the GDPR. Examples are the material scope of application (Article 2 FADP), the obligation to provide information (Article 19 FADP), the right of access (Article 25 FADP), and the existence of criminal sanctions for individuals (Article 60 ff. FADP). The definition of personal data requiring special protection also goes slightly further than it does under the GDPR.

Territorial scope of application of the revised FADP

Although the FADP applies primarily to the territory of Switzerland, it has an extraterritorial scope of application. In particular, it can extend to processing that occurs abroad but has an effect in Switzerland. Consequently, if personal data is processed outside of Switzerland but affects natural persons in Switzerland, the controller or processor abroad must comply with the revised Swiss law. In addition, private controllers with their domicile or residence abroad must designate a representative in Switzerland if they process personal data of persons in Switzerland and the data processing meets all of the following requirements.

- The data processing is connected to offering goods or services in Switzerland or to monitoring the behaviour of these persons.
- The processing is extensive.
- It is a regular processing.
- The processing involves a high risk for the personality of the data subjects.

The representative keeps the records of processing activities, and serves as a point of contact for data subjects and the FDPIC. The controller must publish the name and address of the representation.

Key changes in the revised FADP

Many of the changes in the revised DPA are inspired by the GDPR and will look familiar to data protection experts who have been working with the GDPR. The following changes in respect to the former (current) FADP should be noted.

Sensitive personal data

The list of sensitive personal data (data that requires special protection) has been expanded. The FADP also includes data on ethnicity, genetic data and biometric data that identifies a natural person, but also data relating to the intimate sphere of the data subject and data on social security measures.

Profiling

The revised FADP includes a legal definition of profiling that is identical to that of the GDPR, but there is also "high risk profiling", a special category of profiling with slightly tighter restrictions.

Privacy by design and privacy by default

The principles of "privacy by design" and "privacy by default", which can be found in the GDPR, are introduced in the FADP.

Data protection adviser

Data controllers may, but are not obliged to, appoint an independent data protection adviser as a point of contact for data subjects and authorities responsible for data protection in Switzerland. The tasks of the data protection adviser consist of educating and advising the data controller on data protection issues and assisting in the compliance with data protection legislation.

Records of processing activities

Like the GDPR, the FADP requires that data controllers and processors keep an inventory (records of processing activities or "ROPAs"). This inventory is intended to record the various processing activities of a company and provide the controller and the processor with an overview of the data protection-relevant activities in the company. If the Federal Data Protection and Information Commissioner (FDPIC) investigates a case, the first thing they will likely ask for is the inventory of processing activities. The FDPIC can therefore request this inventory at any time, even if they are not obliged to do so. The minimum content of the inventory is specified in the FADP, and is largely identical to the content required for ROPAs under the GDPR. The Data Protection Ordinance provides for exceptions from the obligation to keep an inventory of processing activities. An inventory does not have to be kept if a company has fewer than 250 employees (as of 1 January). The number of employees is determined per headcount, not FTE, and part-time employees as well as trainees, for example, are fully counted. However, there are "counter-exceptions" in the Ordinance. This means that a company must keep an inventory even though it has fewer than 250 employees if it either:

- carries out extensive processing of particularly sensitive personal data. This includes, for example, organisations and companies whose very purpose entails the processing of particularly sensitive personal data; or
- carries out high-risk profiling, meaning a profiling that entails a high risk for the privacy or the fundamental rights of the data subject by combining data that allows an assessment of essential aspects of the personality of a natural person.

Processing regulations

Although Swiss law does not recognise any general accountability as found in the GDPR, the obligation to have data processing regulations serves the same purpose. The Data Protection Ordinance requires private data controllers and their processors to maintain data processing regulations for automated processing if they either process sensitive personal data on a large scale or carry out high-risk profiling.

According to the Ordinance, the processing regulations must include information on the internal organisation, the processing and control procedures as well as the measures to ensure subject rights and data security. Processing regulations can be in the form of a summary document that references existing documents, directives and guidelines.

Working with data processors

Controllers must enter into a processing agreement with data processors. The FADP requires less for these agreements than the GDPR, but failure to enter into a processing agreement may potentially be liable to criminal sanctions (see below).

Cross-border disclosure of personal data

Like the GDPR, the FADP restricts transfers abroad to countries without adequate protection. Transfers are permitted based on safeguards, which include the standard contractual clauses, which must be adapted slightly to account for Swiss law. In line with the GDPR, the exporter must carry out a transfer impact assessment before commencing a transfer to a recipient in an unsafe country.

Obligation to provide information

Under the FDPA, and similar to the GDPR, the controller must inform the data subjects about its identity, contact details, the purpose of the processing, the recipients or categories of recipients of the data and transfers abroad. In this respect, it requires a list of all countries, including countries with adequate protection, but in practice, privacy notices frequently refer to regions (such as "EEA") instead of listing individual countries. The FADP does not provide a finite list of the required information and, depending on the circumstances, additional information may be necessary. Failure to provide the required information accurately can lead to criminal sanctions.

Automated individual decision-making

Controllers have an obligation to provide information in relation to decisions based solely on automated data processing that have legal consequences or otherwise significantly affect data subjects. In addition, the subjects have a right to voice their view and ask an individual to review the decision. The required information can be included in a privacy notice or can be given when the decision is communicated to the data subject.

Data protection impact assessment

The data protection impact assessment (DPIA) is an important tool for companies to assess data protection risks early, during the implementation of new processes or applications and to take appropriate countermeasures. If a planned data processing activity may involve a high risk to the privacy or the fundamental rights of data subjects, data controllers from the private and public sector must carry out a prior DPIA. This may be the case, for example, with systematic surveillance, processing of confidential or highly personal data, high-risk profiling, or automated decision-making. If a DPIA reveals that the planned processing activity still results in a high risk, despite mitigating measures, the controller must consult with the FDPIC ahead of the processing (unless a data protection adviser is appointed and has been consulted). DPIAs must be kept for at least two years beyond the duration of the processing activity.

Notification obligation of data security breaches

The controller must notify the FDPIC of any data security breach that is likely to result in a high risk for the data subjects – this threshold for the notification obligation is higher than under the GDPR. The notification must be made as soon as possible, but there is no 72-hour maximum

time like under the GDPR. In addition, where necessary for the protection of the data subjects or on instruction by the FDPIC, the controller must inform the data subjects of the breach. According to the Data Protection Ordinance, the notification of a data breach to the FDPIC must contain certain information, in particular the type of breach, the time and duration of the breach, the categories and approximate number of personal data concerned, the categories and approximate number of data subjects concerned, the consequences for the data subjects (including any risks), measures taken or planned, and the name and contact details of a contact person. If it is not possible for the data controller to report all this information at the same time, the controller shall provide the missing information as soon as possible.

Logging obligations

A private controller and/or processor must at least log the storage, modification, reading, disclosure, deletion and destruction of the data (including the identity of the person who carried out the processing, the type, date and time of processing), if sensitive personal data is processed automatically on a broad scale or if a high-risk profiling is carried out and preventive measures cannot guarantee data protection. These logs must be accessible only to relevant functions and may be used only for compliance and security.

Data subject rights

Under the FDPA, data subjects have a range of rights, such as a right to access their data, to have incorrect data rectified, to have automated individual decisions reviewed by a human, and to have their data provided to them or another controller in a common, machine-readable format. Data subjects can also withdraw consent and/or object to the processing of their data, resulting in an obligation on the controller to justify further processing, for example by prevailing interests, or archive or delete personal data. The procedure to follow in the event of a subject request is similar but not identical to that under the GDPR, due to slightly different obligations for timing and more generous exemptions.

Administrative measures and sanctions

Under the FADP, the FDPIC can issue binding orders. These include orders to cease processing, or to destroy personal data or cease disclosure abroad, as well as orders to carry out a data protection impact assessment or give information to a data subject.

The revised FADP has also introduced criminal sanctions of up to CHF250,000 in the event of an intentional breach (including contingent intent) of certain provisions, for example in case of a breach of the information obligation, or incomplete or inaccurate information in case of a subject access request, or where a controller uses a processor without entering into a processing agreement. These sanctions are directed against the individual responsible for the breach (including members of the management, but not limited to them).

Third countries with an adequate level of data protection

Like under the GDPR, there are third countries that benefit from an adequacy decision and which are therefore considered as guaranteeing an adequate level of personal data security. The Federal Council determines these countries, which are listed in Appendix 1 of the Data Protection Ordinance. The list is similar to the adequacy list kept by the European Commission, but there are differences (for example, Japan is not considered to provide adequate protection).

Recommendations

Companies that have not already done so should implement all measures and corrective actions that are required to comply with the revised FADP, as soon as possible. While the level of enforcement in Switzerland continues to be lower than under the GDPR, risks have increased and will likely continue to increase.

Hot Topic Two: AI

Like in the rest of the EU – or the world – the rise of AI, and in particular generative AI, is a hot topic in Switzerland. While Switzerland currently has no specific AI regulations (aside from light-weight regulation for federal authorities), it is closely monitoring the developments in the EU and globally. The Swiss Federal Council has instructed the Federal Department of the Environment, Transport, Energy and Communications to prepare an overview of potential regulatory approaches to AI, which is expected to be available by the end of 2024.

For the time being, data protection remains the key regulation for AI, aside from intellectual property and the protection of business secrets and obligations of professional secrecy. There are no data protection regulations specifically aimed at AI, but the general principles remain applicable, as well as requirements for contracts with providers or customers and with cross-border data transfer restrictions. There is an emerging understanding of how these issues should be tackled in relation with the use of (generative) AI, as well as an understanding of how AI governance should be addressed by companies.

Hot Topic Three: Introduction of Cyber-Attack Reporting Obligation

Cyber-attacks on organisations in Switzerland continue to be on the rise. The manufacturing industry and financial service providers remain a particular focus for cyber criminals. In addition to ransomware, the National Cyber Security Centre of Switzerland (NCSC) records high potential damages to companies with respect to invoice manipulation fraud (business email compromise). The relevance of cyber-risk awareness is therefore increasing in all organisations. There is also a high level of awareness of cyber-risks in Switzerland's management bodies.

Introducing a reporting obligation for cyber-attacks on critical infrastructure and anchoring the NCSC as the national reporting office are seen as additional important steps to improve Switzerland's cybersecurity. Therefore, the new Information Security Act, which is aimed at federal authorities and entered into force on 1 January 2024, will be revised to include a reporting obligation on operators of critical infrastructures and will set out the tasks of the NCSC in this regard, which is intended to act as the central reporting office for cyber-attacks. The revision is expected to come into force on 1 January 2025.

The reporting obligation will apply to operators of critical infrastructures, including, for example, providers in the energy, financial services, healthcare, transportation, telecommunications, search engines and cloud services, and others. Reportable incidents include cyber-attacks that have the potential to cause significant damage. Specifically, these are attacks that endanger the proper functioning of critical infrastructure or are associated with extortion, threats or coercion.

Additional incident notification obligations exist under the FADP (see above) and may apply, depending on the circumstances, for regulated companies such as financial institutions, telecommunications providers, providers of medical devices, and for listed entities.