Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Switzerland
Walder Wyss Ltd

chambers.com

2019

Law and Practice

Contributed by Walder Wyss Ltd

Contents

1. Basic National Legal Regime p.4
- 1.1 Laws p.4
- 1.2 Regulators p.4
- 1.3 Administration and Enforcement Process p.4
- 1.4 Multilateral and Subnational Issues p.5
- 1.5 Major NGOs and Self-Regulatory Organisations p.5
- 1.6 System Characteristics p.5
- 1.7 Key Developments p.5
- 1.8 Significant Pending Changes, Hot Topics and Issues p.6

2. Fundamental Laws p.6
- 2.1 Omnibus Laws and General Requirements p.6
- 2.2 Sectoral Issues p.7
- 2.3 Online Marketing p.8
- 2.4 Workplace Privacy p.8
- 2.5 Enforcement and Litigation p.9

3. Law Enforcement and National Security Access and Surveillance p.9
- 3.1 Laws and Standards for Access to Data for Serious Crimes p.9
- 3.2 Laws and Standards for Access to Data for National Security Purposes p.10
- 3.3 Invoking a Foreign Government p.10
- 3.4 Key Privacy Issues, Conflicts and Public Debates p.10

4. International Considerations p.10
- 4.1 Restrictions on International Data Issues p.10
- 4.2 Mechanisms That Apply to International Data Transfers p.10
- 4.3 Government Notifications and Approvals p.10
- 4.4 Data Localisation Requirements p.10
- 4.5 Sharing Technical Details p.10
- 4.6 Limitations and Considerations p.11
- 4.7 "Blocking" Statutes p.11

5. Emerging Digital and Technology Issues p.11
- 5.1 Addressing Current Issues in Law p.11

6. Cybersecurity and Data Breaches p.11
- 6.1 Key Laws and Regulators p.11
- 6.2 Legal Requirements p.12
- 6.3 Key Multinational Relationships p.12
- 6.4 Data Breach Reporting and Notification p.12
- 6.5 Ability to Monitor Networks for Cybersecurity p.12
- 6.6 Cyberthreat Information Sharing Arrangements p.13
- 6.7 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation p.13

Walder Wyss Ltd has a data protection team of about ten members. In addition, attorneys from other teams provide advice on data protection issues related to their practice areas. Data protection advice has traditionally been a very strong practice area at Walder Wyss, reaching back more than 25 years. Walder Wyss advises major Swiss and international clients in all data protection matters, including the GDPR, and regularly represents clients before the Swiss Data Protection and Information Commissioner as well as before courts. All six office locations are fully integrated, allowing the firm to provide high-quality data protection advice throughout Switzerland and in all national languages. We have a strong international network when it comes to matters which require advice on foreign data protection laws.

Authors

Jürg Schneider is a doctor iuris, Attorney at Law, and a partner, co-head of the data protection team 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 contexts. In addition, Jürg Schneider regularly publishes and lectures on ICT topics, is a member of several professional organisations and co-editor of a website providing comprehensive information on Swiss data protection law. He is a member of the board of directors of the International Technology Law Association and immediate past co-chair of its data protection committee. Jürg Schneider's special competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of GDPR (and the future revised Swiss DPA) for Swiss and international companies, advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements, among others.

David Vasella is a doctor iuris, Attorney at Law, CIPP/E, partner and co-head of the data protection team. David advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. He deals with cross-jurisdictional data projects including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. David also regularly advises in relation to commercial IP matters, regulated products, and market practices. In addition, David frequently speaks and publishes in his area of expertise. He is an editor of the Swiss journal for data law and information security and a member of the professional bodies IAPP and DGRI.

Hugh Reeves is an Attorney at Law and an associate in the Information Technology, Intellectual Property and Competition Team. He pursued a further education degree (LLM) at the University of California at Berkeley where he specialised in the intersection of law and technology before gaining additional professional experience within a leading Silicon Valley law firm. Hugh Reeves' preferred areas of practice include technology transfers, information technology law, data protection, as well as copyright, patent, trade mark and trade secret law. He is registered with the Vaud Bar Registry and admitted to practise throughout Switzerland. Hugh has contributed to many publications relating to data protection law.

1. Basic National Legal Regime

1.1 Laws

On a federal level, the Swiss Constitution of 18 April 1999 protects the right to privacy, in particular the right to be protected against misuse of personal data (Article 13). The collection and use of personal data by private bodies are regulated on a federal level and are mainly governed by the Federal Data Protection Act of 19 June 1992 (the 'FDPA') and its ordinances, including the Ordinance to the Federal Act on Data Protection (the 'FDPO'). Data processing by public bodies is governed by the FDPA for federal bodies and by cantonal (for example, the Information and Data Protection Act of the Canton of Zurich) and communal laws for cantonal and communal bodies.

The FDPA is currently under revision in order to implement the revised Council of Europe's Convention 108 and to align with the EU General Data Protection Regulation (GDPR). The Federal Council published a proposal for the revised FDPA on 15 September 2017 and initiated a consultation process. At the issue of this consultation process, the Federal Council decided to split the revision process into two separate phases. A first phase targeted the necessary amendments to bring Swiss legislation in line with changes to the Schengen/Dublin framework (EU Directive EC 2016/680 of 27 April 2016). These changes were made and implemented in a Federal Council decision of 30 January 2019 and will enter into force on 1 March 2019. During a second and still ongoing phase, Parliament will discuss the draft of the revised FDPA. Given these latest developments, no final wording of the revised FDPA is available as yet. There is a general expectation that the revised FDPA will not enter into force before 2020 or 2021.

A number of provisions in other laws restrict or allow the processing of personal data, in particular in the public sector (for example, in mandatory health insurance) and in regulated markets (for example, for banks and insurance companies). These laws include:

- in the healthcare and medical sectors – the Federal Act on the General Part of Social Insurances contains general as well as specific provisions on the health insurance sector and includes provisions on confidentiality and the authorised extent of data processing in the governed context. Another noteworthy piece of legislation is the Federal Human Research Act and its related ordinance, which both contain detailed rules on the storage of personal data as well as the Federal Act on Electronic Patient Files;
- in the banking and finance sectors – the Federal Banking Act (the 'Banking Act') outlines banking secrecy, though the impact of this provision has somewhat lessened over the past decade. The Federal Act on Financial Market Infrastructure ('FinfrAct') in particular sets out rules on IT systems, emergency responses and other business continuity. The Federal Stock Exchange Act ('SESTA') contains confidentiality obligations. On a more specific level, the Swiss Financial Market Supervisory Authority (FINMA) issued various circulars that contain precise data security requirements (notably FINMA Circular 2008/21 on operational risks); and
- the Federal FTA (the 'FTA') and the Ordinance on Telecommunications should be mentioned. Articles 43 et seq of the FTA contain data protection requirements and provide for telecommunication secrecy.

There is no dedicated cybersecurity legislation in Switzerland to date. Cybersecurity is regulated by a patchwork of various Acts and regulatory guidance, which deal explicitly or implicitly with cybersecurity in the private sector. These laws include:

- the Budapest Convention on Cybercrime, which entered into force in Switzerland on 1 January 2012;
- the FDPA;
- the FTA; and
- the FinfrAct.

1.2 Regulators

The Federal Data Protection and Information Commissioner (FDPIC) is a body established on a federal level under the FDPA. The FDPIC supervises compliance with the FDPA and other federal data protection legislation by federal bodies, and advises private bodies. On its own initiative or at the request of a third party, the FDPIC may carry out investigations into data processing by private bodies if their data processing is capable of affecting a large number of persons. In addition, each canton has its own data protection authority, which is generally competent to supervise cantonal and communal bodies (but not private parties, which are subject to the FDPIC's authority).

Other regulators, for example the FINMA, may play a role in the enforcement of data protection (see below).

1.3 Administration and Enforcement Process

The FDPA sets out basic rules applicable to investigations carried out by the FDPIC.

The FDPIC has no direct enforcement powers against private bodies processing personal data. However, on its own initiative or at the request of a third party it can carry out investigations if a suspected privacy breach is capable of affecting a large number of persons ('system error') and in limited additional cases. In the course of an investigation, the FDPIC has the right to demand the production of documents, make inquiries and ask for a demonstration of a particular processing of personal data. However, under the current FDPA the FDPIC cannot issue binding instructions to the data handler, though this is due to change under the

revised FDPA. The FDPIC's only instrument at this stage is issuing a non-binding recommendation to change or terminate a processing activity. If the recommendation is not followed, the FDPIC may refer the matter to the Federal Administrative Court for a decision on the subject matter of the recommendation. This Federal Administrative Court's decision is binding but can be appealed before the Federal Supreme Court. Neither these courts nor the FDPIC can impose monetary sanctions, but they can refer the matter for criminal prosecution, which may lead to a fine of up to CHF10,000 in very limited scenarios.

The investigation by the FDPIC is subject to the Federal Act on Administrative Procedure (APA), which provides for due process rights for the investigated party and third parties, for example rights to refuse to testify. The procedure before the Federal Supreme Court is regulated by the Federal Act on the Supreme Court.

1.4 Multilateral and Subnational Issues

Switzerland has implemented the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') through the FDPA, and is currently in the process of revising the FDPA to follow the revision of Convention 108. In addition, Switzerland is not a member of the EU or of the EEA and under no obligation to implement the EU General Data Protection Regulation (GDPR), but the EU is Switzerland's most important partner, and ensuring a level playing field for Swiss and EU-based companies is an important policy objective. The current revision of the FDPA therefore largely aligns with the GDPR and while there is no final draft to date, it is expected that the revised FDPA will be compatible with the GDPR such that a company that complies with the GDPR should generally be in compliance with the revised FPDA. Moreover, it is expected that the European Commission will maintain its finding that Switzerland's data protection legislation provides an adequate level of data protection under the GDPR.

For data processing in relation to criminal prosecution, and in the framework of police and judicial co-operation, Switzerland transposed, on 30 January 2019, EU Directive 2016/680 into domestic Swiss legislation through the revision of the FDPA. It expedited the adoption of this piece of legislation, with the relevant changes becoming effective on 1 March 2019.

1.5 Major NGOs and Self-Regulatory Organisations

The FDPA does not provide an official role for NGOs and SROs. Such organisations would not, for example, have a right to bring a civil claim against a company perceived to be in breach of privacy laws. However, there are a number of organisations that promote privacy, including several consumer protection organisations. Furthermore, NGOs and SROs may request the FDPIC to open investigations if a suspected privacy breach is capable of affecting a large number of persons ('system error') and in limited additional cases.

1.6 System Characteristics

Swiss data protection law, in particular the FDPA, is partly based on Convention 108 and is generally similar to European data protection legislation. However, there are a number of differences.

Under the FDPA, processing by private companies does not require legal grounds, as long as the fundamental processing principles are complied with. These include legality, acting in good faith, transparency, purpose limitation, proportionality, correctness and data security. In the event of a breach of these principles, however, processing is lawful only if it is justified by a Swiss law requiring processing, by valid consent of the affected data subjects, or by a prevailing Swiss public or private interest.

In contrast to the relevant laws of most European countries, the FDPA protects information pertaining to legal entities much in the same way it protects information pertaining to individuals. The FDPIC therefore considers that a disclosure of information pertaining to legal entities to countries without such protection requires adequate safeguards.

There is a general view that enforcement of the FDPA has been inadequate in the past. This is one of the drivers of the ongoing revision of the FDPA. This perceived lack of enforcement is due to several factors, including:

- the FDPIC has no direct enforcement powers against private bodies processing personal data (see above) and, with limited resources, typically concentrates on data processing by federal bodies and, in the private sector, on significant or high-profile cases;
- there is no risk of criminal sanctions for a breach of data protection laws, except in very limited scenarios; and
- in the event of a breach of data protection law, there is a risk of civil liability towards the concerned data subjects and, depending on the circumstances, a risk of negative publicity. However, there is normally no financial risk as claims for compensation with the required data are subject to establish financial losses. There is no claim for compensation of non-material damage, in contrast to the GDPR.

1.7 Key Developments

The main developments over the past 12 months have concerned ongoing revision of the FDPA. As mentioned above, the Federal Council decided to split the revision process into two phases. Regarding the first step, Switzerland transposed, on 30 January 2019, EU Directive 2016/680 into domestic Swiss legislation. Regarding the actual total revision of the FDPA, Parliament – or, more specifically, the Political Insti-

tutions Committee of the National Council (lower house) – decided, in winter 2018, to discuss the revision of the FDPA in the first quarter of 2019. In effect, compared to the situation a year ago, the timeline of the revision process has seen an extra year added. This delay means that entry into force of the revised FDPA will not take place before 2020 or 2021. That being said, it is expected that the final text of the revised FDPA will be in line with the GDPR.

Another development has been in the field of social insurances. Indeed, in a 25 November 2018 referendum, the Swiss people voted in favour of a proposed change to the social insurance legislation, allowing social insurance providers to monitor, under certain conditions, insurance claimants in cases of suspected insurance fraud. This monitoring may also be performed undercover. These changes, which are not yet in effect (no known date at the time of writing) were triggered by a decision of the European Court of Human Rights (ECHR) of 18 October 2016 whereby the ECHR ruled that Switzerland did not have a sufficient legal basis to perform (undercover) monitoring of social insurance claimants.

1.8 Significant Pending Changes, Hot Topics and Issues

See **1.7 Key Developments**.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The key requirement under the FDPA is to comply with the general principles it has established, ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security. Some of these principles are specified in more detail in the FDPA and the FDPO, for example data security requirements.

The FDPA generally applies a light-touch approach and imposes limited governance obligations on private players. For example, the FDPA does not require private companies to appoint a data protection officer (DPO). For this reason, DPOs have not played an important role in Switzerland compared with other countries.

Compliance with the fundamental processing principles already suffices for the collection and other processing of personal data. These include legality, acting in good faith, transparency, purpose limitation, proportionality, correctness and data security. In the case of a breach of these principles, however, processing is lawful only if it is justified by a Swiss law requiring processing, by valid consent of the affected data subjects, or by a prevailing Swiss public or private interest.

There are no specific privacy by design and privacy by default obligations. However, such obligations may arise by implication under the principle of proportionality and data security, depending on the risk profile of the particular processing activity.

There is no requirement for private companies to carry out a data protection impact assessment. However, such obligation may arise by implication under the principle of proportionality.

There is no express requirement to adopt privacy policies, even though most larger companies will and should have a privacy policy or code of conduct. However, a privacy notice (privacy statement) is necessary if the processing would not reasonably be expected by the data subjects and is not required under statutory laws, and whenever sensitive personal data or personality profiles are collected.

Data subjects have certain rights under the FPDA, including:

- the inalienable right to access information about themselves. Upon request, the controller of data collection must inform the data subject in writing whether he or she processes personal data about the data subject making the request and provide additional information about the processing;
- the right to require that incorrect personal data is rectified by modifying, (partially) deleting or complementing the data on record;
- the right to require that personal data is deleted, provided that the party processing the data has no prevailing interest in the processing; and
- the right to require that personal data is not disclosed to third parties.

The FDPA does not currently provide for a data portability right.

The FDPA and the FDPA do not define 'pseudonymous' or 'anonymous data.' However, both are important elements of data security that have been recognised and recommended by the FDPIC in guidance on technical and organisational measures issued in August 2015. Anonymous data is data that no longer relates to an identified or identifiable person. Processing of anonymous data does not fall under the FDPA. However, the act of anonymising personal data is subject to the rules set out in the FDPA.

The FDPA defines so-called 'personality profiles,' which means a collection of data that allows an assessment of essential characteristics of the personality of a natural person. The FDPA contains a number of provisions establishing more restrictive rules for these data categories, for example:

- data subjects must be actively informed that sensitive data/personality profiles will be collected;

- disclosure of sensitive data or personality profiles to a third party (excluding processors) requires consent or another justification; and
- when consent is relied on for processing these data categories, consent must be given explicitly to be valid.

It should be noted that federal bodies can only process personality profiles in limited cases.

Swiss data protection law does not define injury or harm. Any potential injury or harm, whether material or non-material, must be taken into account when assessing risk for the data subjects, or when balancing interests. However, there is in general no claim for financial compensation for injury or harm unless there is quantifiable financial damage.

2.2 Sectoral Issues

'Sensitive personal data' as defined in the FDPA means data on religious, ideological, political or trade union-related views or activities, health, the intimate sphere or racial origin, social security measures, or administrative or criminal proceedings and sanctions. An additional category of data that benefits from increased protection is the 'personality profile' as detailed above.

Financial data

Several laws in the financial sector contain provisions on dealing with data. Under the Banking Act, it is a criminal offence for an employee, agent or representative of a bank to disclose any information in which they have been confided or which they become aware of in the course of their professional role without their client's authorisation, unless an exemption applies. Similar restrictions apply to securities dealers under the Federal Stock Exchange and Securities Act, the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading and the Collective Investment Schemes Act.

Health data

The Federal Act on Research on Humans, the Federal Act on Human Genetic Testing, the Federal Ordinance on Health Insurance and the Federal Act on Electronic Patient Files set out specific restrictions and requirements on the processing of health-related data. Moreover, doctors and certain other members of the medical profession are bound by a duty of professional secrecy under the Criminal Code.

Communications data

The Federal Telecommunications Act (FTA) sets forth confidentiality obligations on telecommunications service-providers, which apply in addition to the FDPA. Disclosing information relating to subscribers' communications to a third party without consent amounts to a criminal offence.

The FDPA defines sensitive data as data on religious, ideological, political or trade union-related views or activities, health, the intimate sphere or racial origin, social security measures, administrative or criminal proceedings and sanctions.

There is no express obligation to post a privacy notice on a website. However, the transparency principle under the FDPA requires a notice if the processing cannot reasonably be expected and is not required under statutory laws, and privacy notices are posted on most websites. However, any person that offers goods or services through electronic channels, including on a website, must indicate its name and contact details, including an email address under the Federal Unfair Competition Act ('Unfair Competition Act'). When goods or services are sold through electronic channels the seller must provide additional information and must send an order confirmation.

Use of cookies, beacons, tracking technology

Under the FTA, using cookies and other technologies that store personal data on a device is only permitted if the user is informed about the processing and its purpose and how they can reject cookies (opt-out). This applies regardless of the purpose and type of cookies or other technology, including session cookies and tracking cookies. Failure to provide the required information may lead to a fine of up to CHF5,000.

"Do not track" considerations

There is no obligation on software providers to include or activate by default a 'do-not-track' option. However, in the view of the FDPIC an activated do-not-track option is binding on website providers.

Consent required for behavioural advertising

As mentioned above, processing of personal data is generally lawful if it is in accordance with the general principles set forth in the FDPA. Consent is therefore not required unless one of the principles is not complied with. As a general rule, therefore, behavioural advertising is permitted without consent if the data subjects are notified about the advertising in a privacy notice. However, restrictions and requirements under the FTA regarding the use of cookies as well as under the Unfair Competition Act as regards electronic mass advertisements must be complied with (see below).

There are no laws specifically targeting technologies such as social media, search engines and online platforms. The key Regulations in this area are the FDPA and the Unfair Competition Act, and liability is primarily subject to the Swiss Civil Code and the Swiss Code of Obligations ('Code of Obligations'). With respect to their obligation to prevent infringements, the liability of online platform providers and intermediaries is not fully clear. However, providers are generally not responsible for monitoring traffic for illegal content, but if they are notified of illegal content they are under an obligation to block access to or remove such content.

Right to Be Forgotten (or of Erasure)
With respect to the right to be forgotten, the FDPA requires any person processing personal data to erase the data when keeping the data is no longer required for the processing purpose or for compliance with a legal obligation, and if the data subject asks for erasure and no statutory retention obligation or prevailing Swiss public or private interest overrides the request.

Addressing Hate Speech, Disinformation, Abusive Material, Political Manipulation, etc
The Swiss Criminal Code ('Criminal Code') prohibits various forms of discrimination against persons by private individuals on the basis of their race, ethnicity or religion, whether in the form of photos, videos, pictures or text, provided that the communication is in the public domain, ie, if the target audience is not limited to persons who are connected by a relationship of trust. Discrimination based on other characteristics such as gender, age or sexual orientation is not a criminal offence, but may infringe on personality rights.

Disinformation and political manipulation is generally not a criminal offence, as long as it does not use force or threats, and will in most cases not be caught by the Unfair Competition Act.

Data portability
There is no right to data portability under the current FDPA or other laws, and it is expected that the revised FDPA will not provide for such a right.

Children's Privacy
Personal data of children and adults is protected in the same way under the FDPA. There are no special rules in this regard and no set age threshold for valid consent. Consent may be provided by children when they are old enough to understand the scope of the processing in question and the impact of their consent.

Educational or school data
There is no regulation targeted at education or school data, and such data does not constitute sensitive data. The general provisions of the FDPA will apply to such data, and cantonal privacy laws apply to cantonal and communal authorities, including public schools dealing with such data.

2.3 Online Marketing

Under the Unfair Competition Act, electronic mass-marketing communication (including emails and SMS, but also cold calling) is permitted only with the recipient's consent unless it is sent to existing customers and provided that certain cumulative conditions are met, which include:

- the sender obtained the customer's contact information at the occasion of the purchase of a product, service or works;
- the sender had informed the customer, when obtaining his or her personal information, about the possibility to opt out from direct marketing;
- the marketing communication refers to own and similar products, services or works, of the sender that the customer has purchased in the past;
- the sender provides its correct and complete contact information (including address); and
- the sender provides a reference to an easy, free of charge option to refuse future marketing materials.

Additionally, providers of telecommunications services must address unfair mass advertising under the FTA.

Subscribers can have their telephone numbers marked to indicate that they do not wish to receive marketing calls. Making unsolicited marketing calls to such numbers or sending marketing messages by fax or email is prohibited under the Unfair Competition Act.

There are no constraints specifically on behavioural advertising. The general rules (the FDPA, Unfair Competition Act and the FTA) apply.

There are no constraints specifically on location-based communication, including advertising. The general rules (the FDPA, Unfair Competition Act and FTA) apply.

2.4 Workplace Privacy

The Code of Obligations applies to the processing of personal data of employees in addition to the FDPA.

According to the Code of Obligations, employers must not process personal data relating to an employee if such personal data does not concern the employee's suitability for his or her job or is necessary for the performance of the employment contract. Moreover, Ordinance 3 to the Labour Act prohibits the use of systems that monitor the behaviour of employees, except if such monitoring systems are necessary for other legitimate reasons and do not negatively affect the health and mobility of employees.

The FDPIC has issued specific guidelines on the processing of employee data.

Certain key requirements apply to the monitoring of internet and email use by employees, including:

- the employer should describe the permitted use of company internet and email resources by employees;
- permanent personally identifiable analysis of log files is prohibited;
- permanent anonymous analysis of log files and random pseudonymised analysis are admissible for the purpose of verifying that the acceptable use policy is complied with;

- an individual analysis of log files is only allowed if the employee has been informed in advance of this possibility and if there is a reason to suspect abuse; and
- the monitoring policy should mention the possibility of an analysis on a personally identifiable basis, that such an analysis may be passed on to the HR department, and potential sanctions.

Employee representatives (or employees, should there be no employee representatives in the particular undertaking) must be informed by their employer about certain matters, which may include employee monitoring systems and whistle-blowing hotlines. There may be a consultation requirement for monitoring systems.

Whistle-blower hotlines are not specifically regulated, but several restrictions apply under the FDPA and the Code of Obligations. However, in the grand scheme of things the situation is similar to that in the EU, and a company in compliance with EU law will normally be in compliance with Swiss law. General rules applicable to the implementation and operation of whistle-blowing schemes in Switzerland include:

- employees should be informed about the existence of the whistle-blowing hotline;
- employees, contractors and other persons should be informed about suspected wrongdoing through the whistle-blowing hotline. However, it will generally be acceptable to delay such information if and for as long as necessary in order not to hamper an ongoing investigation or in order to secure evidence;
- employees should be protected against false or slanderous accusations; and
- state-of-the-art security measures should be applied.

Whistle-blowing hotlines may require prior registration with the FDPIC. In the event of transfers abroad, specific requirements must be met.

2.5 Enforcement and Litigation

As mentioned above, the FDPIC cannot open an investigation unless a suspected privacy breach is capable of affecting a large number of persons and in limited additional cases, including if a mandatory notification to the FDPIC has not been made.

The FDPIC has no right to impose criminal and/or administrative sanctions.

There is a risk of criminal fines issued by the criminal courts in very limited cases, for example when a mandatory notification to the FDPIC is not made, in the case of intentional failure to comply with a data subject's access request, and if sensitive personal data or personality profiles are disclosed to third parties without authorisation or if such data is collected without authorisation from a non-public data file.

If the Federal Administrative Court issues a binding order, it may impose fines for non-compliance with the order.

As mentioned above, due to a 2016 ECHR decision, Switzerland adapted in 2018 its social insurance legislation, though no date of entry into force is yet known. These changes, once in force, will allow social insurance providers to monitor, under certain conditions, insurance claimants in cases of suspected insurance fraud.

A breach of privacy may give rise to cease-and-desist claims and claims for financial compensation. However, financial claims require the claimant to establish quantified financial damages, which is often not possible. Allegations of a breach of privacy are therefore more often a support to other claims, for example in an employment litigation, than a standalone cause of action.

Class actions are not allowed in Switzerland.

There are no leading or other major cases to report in the last 12 months.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The Federal Act on Intelligence Services and the Federal Postal and Telecommunications Surveillance Act (usually in combination with the Criminal Code and the Swiss Code of Criminal Procedure) constitute the main legislation that law enforcement, prosecution authorities and national security and intelligences services rely on for surveillance purposes.

Various forms of surveillance (such as in public places) and information requests (telecommunications services user identity) do not necessarily require prior judicial approval. More intrusive measures (typically live surveillance and communications interception) do, however, require judicial approval. That being said, in many cases such measures can be carried out secretly, without the data subject's (immediate) knowledge.

As mentioned above, judicial review is at the centre of the array of safeguards legally in place. Moreover, the collected data remains subject to strong purpose limitation by law, including but not limited to the Swiss Code of Criminal Procedure, which limits the scope of evidentiary uses of any data collected throughout a criminal investigation (as may often be the case in surveillance and communications interception).

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

See section **3 Law Enforcement and National Security Access and Surveillance**.

3.3 Invoking a Foreign Government

In the absence of any order emanating from a Swiss court, requests from foreign governments do not allow for the collection and transfer of personal data located in Switzerland.

3.4 Key Privacy Issues, Conflicts and Public Debates

The discussion about government access to personal data focuses on rights of access by US authorities on personal data stored abroad. For example, the US Supreme Court case involving Microsoft and the US CLOUD Act are observed in Switzerland. The possibility of foreign government access is considered to constitute a risk that must be taken into account for Swiss companies evaluating the use of foreign cloud service providers. There is generally less awareness of the right for Swiss authorities to gain access to personal data stored in Switzerland.

4. International Considerations

4.1 Restrictions on International Data Issues

Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection. Personal data may therefore not be transferred outside Switzerland without specific requirements if the recipient's jurisdiction does not ensure an adequate level of data protection. The FDPIC maintains a list of such countries. With regard to personal data related to individuals, all EU and EEA member states are considered to provide an adequate level of data protection.

If personal data is to be transferred to a country without an adequate level of data protection, such a transfer may only occur if:

- sufficient safeguards apply to the transfer, in particular contractual clauses (in practice, usually the EU model clauses adapted to Swiss law requirements);
- the data subject has provided specific, informed consent;
- the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
- the transfer is essential in the specific case either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- the transfer is required in the specific case to protect the life or the physical integrity of the data subject;
- the data subject has made the data generally accessible and has not expressly prohibited its processing; and
- disclosure is made based on binding corporate rules (BCR).

4.2 Mechanisms That Apply to International Data Transfers

Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection. Personal data may therefore not be transferred outside Switzerland without specific requirements if the recipient's jurisdiction does not ensure an adequate level of data protection. The FDPIC maintains a list of such countries. With regard to personal data related to individuals, all EU and EEA member states are considered to provide an adequate level of data protection.

If personal data is to be transferred to a country without an adequate level of data protection, such a transfer may only occur if:

- sufficient safeguards apply to the transfer, in particular contractual clauses (in practice, usually the EU model clauses adapted to Swiss law requirements);
- the data subject has provided specific, informed consent;
- the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
- the transfer is essential in the specific case either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- the transfer is required in the specific case to protect the life or the physical integrity of the data subject;
- the data subject has made the data generally accessible and has not expressly prohibited its processing; and
- disclosure is made based on binding corporate rules (BCR).

4.3 Government Notifications and Approvals

In the case of a transfer based on safeguards (or BCR), the FDPIC must be informed in advance. If a recognised model agreement is used, there is no requirement to submit the agreement to the FDPIC.

4.4 Data Localisation Requirements

With a few exceptions (for example, the Federal Act on Electronic Patient Files), there are no data localisation requirements under Swiss law.

4.5 Sharing Technical Details

No software code or algorithms or similar technical detail are required to be shared with the government.

4.6 Limitations and Considerations

'Blocking statutes' may prohibit the transfer of data (personal data and otherwise) abroad. Article 271 of the Criminal Code prohibits certain activities on behalf of a foreign state. These include assisting foreign official proceedings through actions within the borders of Switzerland, such as collecting data on behalf of foreign authorities. This provision does not prohibit data transfers abroad where the transfer is not intended to assist in a foreign procedure and is not made upon the instruction of a foreign authority or is made in accordance with rules on international judicial assistance. There is the potential to request authorisation to perform acts for a foreign state on Swiss territory. Authorisation will be issued by the competent federal department, or in cases of greater magnitude with political or fundamental significance by the Federal Council.

4.7 "Blocking" Statutes

In addition to Article 271 of the Criminal Code noted above, anti-disclosure provisions in Article 273 of the Criminal Code prohibit the disclosure of secrets to official or private foreign bodies or private foreign companies. In cases where only a private Swiss entity has an interest in keeping such trade or business secrets confidential (and not the Swiss Confederation due to national interests) it is up to the relevant entity to decide whether it agrees to the disclosure or not. Its consent prior to the disclosure is sufficient to avoid criminal charges based on Article 273 of the Criminal Code. However, in cases where such secrets are of national interest, or if a third party has a reasonable interest in keeping such secrets confidential from the foreign recipient and does not consent to the disclosure, such trade or business secrets must not be revealed.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

There is no specific regulation on Big Data and related analytics. However, should the data not be fully anonymised (including if the combination of the pseudonymised data allow for re-identification), the provisions of the FDPA will apply. In such circumstances, the general principles of the DPA, in particular purpose limitation, proportionality and transparency, may prove problematic.

There is no specific regulation on automated decision-making under the current FDPA. Such process may run afoul of the general principles of the FDPA, in particular purpose limitation, proportionality and transparency.

The FDPA contains special rules on so-called 'personality profiles,' which are usually the same rules as are applicable to sensitive personal data (see above).

The use of artificial intelligence and machine learning is not specifically regulated, and is subject to the general rules of the FDPA where it involves personal data.

The IoT is not specifically targeted by current Swiss legislation. It may lead to conflicts with the FDPA where cross-border data transfers take place, and data security requirements are not met.

There is no specific regulation on autonomous decision-making. The general principles of the FDPA apply, in particular the principles of transparency, proportionality and purpose limitation.

Facial recognition is not as such regulated under FDPA. However, data processed within the context of facial recognition may be deemed sensitive personal data.

The general rules of data protection apply to biometric data. The FDPIC issued guidance on the use of biometric data in 2010, and a 2009 Federal Administrative Court decision ruled that the centralised storage, by a private company, of biometric data violated the proportionality principle as set out in the FDPA. As this ruling was rendered in a specific situation where the biometric data was linked to other personal data, it cannot be construed as leading to a general ban on centralised storage of biometric data. Therefore, analysis on a case-by-case basis remains necessary going forward.

No specific rules apply to the use of geolocation data. However, such data may often contain personal data, either directly or through re-identification of statistical and other geometrical data. In such situations, the general principles of the FDPA must be complied with, in particular the principles of transparency, purpose limitation and proportionality.

Drones of up to 30kg do not require a permit under current Swiss law, provided however that the pilot does not perform crowd fly-overs and retains permanent visual contact. As drones are frequently equipped with (video) cameras, the general rules of data protection may apply.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

There is no dedicated legislation governing cybersecurity, be it on a federal or cantonal level. The legal governance of cybersecurity therefore falls within the scope of various laws. As mentioned above, the key legislation in this area is the FDPA and the FDPO and the Criminal Code. Sectorial provisions are typically found in the FTA, the Banking Act and FinfrAct.

The key official authorities in the cybersecurity area are MELANI, the Federal cybercrime agency, the Swiss Coor-

dination Unit for Cybercrime Control (CYCO), which is primarily a forwarding and co-ordinating authority for criminal cases, and the FDPIC, which retains strong prerogatives given the absence of stand-alone cybersecurity legislation.

On 30 January 2019, the Federal Council decided in favour of a new competence centre for cybersecurity, which will be managed by a 'cybersecurity delegate.' This competence centre and its delegate will act as a centralised contact point for all matters pertaining to cybersecurity and closely interact with the other players, in particular MELANI. This is an ongoing process as the cybersecurity delegate must still be appointed, but further developments are expected in the course of spring 2019.

As mentioned above, the FDPIC retains a central role in the area of cybersecurity. It can investigate cases brought to its attention and can also do so on its own initiative, within its limited powers noted above. The revised FDPA should bring about stronger enforcement powers for the FDPIC.

The above-mentioned FINMA is the competent authority in the banking and financial sectors. As part of its statutory mission and in the course of supervising regulated financial entities, FINMA may also request compliance with applicable data protection regulations.

The OFCOM is the responsible federal office for the proper implementation of the legal and technical requirements in the communications realm and plays a particularly important role in the area of telecommunications. In the area of unfair competition, the State Secretariat for Economic Affairs (SECO) acts for the Swiss Confederation in civil and criminal proceedings if matters of public interest are at stake.

6.2 Legal Requirements

There are no legally required security standards. However, such standards are often required in contracts such as data processing agreements, and are used by data processors to demonstrate appropriate data security. Typical standards include ISO 27001 and ISO 27018:2014. Moreover, industry associations may adopt specific requirements. For example, the Swiss Bankers Association has issued standards for business continuity and data leakage prevention.

Walder Wyss Ltd

Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

walderwyss

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

There are no express legal requirements for written security plans, the appointment of DPOs, involvement of the board and so on, except that the company laws, namely the Code of Obligations, rules of the FDPA (Article 7), the FDPO (Articles 8-12) and sectorial Regulations (such as FINMA Circular 2008/21 'Operational Risks – Banks') may imply a need for or lead to the implementation of such plans and procedures. For example, the FINMA Circular 2008/21 requires the bank's executive management to implement a risk management concept on how to deal with cyber risk and ensure appropriate business continuity arrangements, and sets out requirements for an appropriate management of risks in relation to the confidentiality of electronic personal data. Moreover, industry associations may adopt requirements, such as the Swiss Bankers Association's standards for business continuity and for data leakage prevention.

6.3 Key Multinational Relationships

Switzerland's commitment to the Budapest Convention on Cybercrime (in effect for Switzerland) and the revised Council of Europe's Convention 108 should be noted.

6.4 Data Breach Reporting and Notification

Currently, data breaches are not subject to specific notification or reporting obligations, although proper data security practices under the FDPA and FDPO (as well as sectorial regulations), combined with the general principle of transparency may of course lead to (the need for) breach notifications. This situation is expected to change under the revised FDPA as it is a matter of compliance by Switzerland with the requirements of the revised Council of Europe's Convention 108.

As an exception to the above, telecommunications service-providers must inform the OFCOM of failures in the operation of their networks that affect a relevant number of customers. Moreover, there are notification obligations in certain sectors in the event of adverse events, which may include data breaches. For example, certain occurrences that endanger an aircraft, its occupants or other persons, or equipment or installation affecting aircraft operations must be notified to the Federal Office of Civil Aviation in accordance with EU Regulation no 376/2014.

6.5 Ability to Monitor Networks for Cybersecurity

See above regarding Law Enforcement and National Security Access and Surveillance. Under certain conditions, and subject to judicial approval, emails and other means of telecommunication can be intercepted and monitored, either live or retroactively. These possibilities have been bolstered through the revision of the Federal Postal and Telecommunications Surveillance Act.

6.6 Cyberthreat Information Sharing Arrangements

Information-sharing has not been specifically regulated. Proper cybersecurity practices may call for such information-sharing, though such assessment needs to be done on a case-by-case basis as it may entail the processing of personal data.

6.7 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

In recent years, the most noteworthy case arose when it appeared, in 2016, that the Swiss defence company RUAG had suffered from cyber-espionage and lost a significant quantity of data. The MELANI, upon the decision of the federal government, published its findings enabling other organisations to take remedial or pre-emptive measures.