Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

Switzerland
Pestalozzi

chambers.com

2020

SWITZERLAND

Law and Practice

Contributed by:
Lorenza Ferrari Hofer and Michèle Burnier
Pestalozzi see p.14

Contents

1. Basic National 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 Federal Act on Data Protection of 19 June 1992 (the Data Protection Act, the DPA) and the Ordinance to the Federal Act on Data Protection of 14 June 1993 (ODPA) are the major laws in this field.

The DPA is currently undergoing a total revision in order to align with the EU General Data Protection Regulation (GDPR). The Federal Council published a proposal for the revised DPA on 15 September 2017 and this is still before the Swiss Parliament. In November 2019 the Council of States debated the totally revised DPA and adopted most of the improvements proposed by its Commission in comparison to the National Council version. Thus, there seems to be nothing to prevent further finalising consultations in the spring session 2020. Given the latest developments, the revised DPA will not enter into force before 2021 or 2022.

Data processing by federal public bodies is governed by the DPA. In addition, every Swiss canton has its own data protection statutes with respect to data processing by cantonal public bodies (including the communes).

Finally, a number of provisions in other laws restrict or allow the processing of personal data, in particular in the following sectors:

- labour laws – restriction of the possibility of monitoring employees;
- healthcare insurance – the Federal Act on the General Part of Social Insurances, the Federal Act on Health Insurance, and the Federal Act on Electronic Patient Files are among the most relevant pieces of legislation;
- human research – the Federal Human Research Act and its related ordinance;
- banking and financial sectors – the Federal Banking Act, the Federal Act on Financial Market Infrastructure and the Federal Stock Exchange Act (in addition, the Swiss Financial Supervisory Authority (FINMA) has issued various circulars dealing with security measures);
- telecommunication – the Federal Act on Telecommunication and its ordinance; and
- the Unfair Competition Act.

There is no dedicated cybersecurity legislation in Switzerland to date.

The key requirement under the DPA 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 DPA and the ODPA; for example, data security requirements. Legal and natural persons have the following rights in relation to the processing of their personal data:

- Right of access to data/copies of data – any person may request information from the Controller of the Data File as to whether data concerning him or her is being processed (see Article 8 paragraph 1 DPA; exceptions are mentioned in Article 9 DPA), the information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge.
- Right to rectification of errors – any data subject may request that incorrect data be corrected (see Article 5 paragraph 2 DPA).
- Right to deletion/right to be forgotten – any data subject may request that incorrect data be deleted (see Article 5 paragraph 2 DPA), the right to be forgotten is not explicitly mentioned in the DPA, but the Federal Data Protection and Information Commissioner (FDPIC) and case law consider that such a right results from the general principle of proportionality.
- Right to object to processing – data subjects may request (in a civil litigation) that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed (see Article 15 paragraph 1 DPA), it is important to note that data processing may be blocked by preliminary injunctions.
- Right to withdraw consent – according to Article 12 paragraph 2 littera b DPA, "anyone must not process data pertaining to a person against that person's express wish without justification", based on this provision, it is possible to withdraw consent at any time.
- Right to object to marketing – in addition to the objection to data processing for marketing purposes as set out above, there is a special regulation regarding mass emails (ie, marketing newsletters) in Article 3 littera o of the Unfair Competition Act.
- Right to complain to the relevant data protection authority(ies) – the FDPIC may investigate cases in more detail on his or her own initiative or at the request of a third party (see Article 29 paragraph 1 DPA).

The DPA defines so-called "personality profiles" (ie, a collection of data that allows an assessment of essential characteristics of the personality of a natural person) as sensitive personal data. The DPA contains a number of provisions establishing more restrictive rules for this data category.

1.2 Regulators

The Federal Data Protection and Information Commissioner (FDPIC) is the relevant supervisory regulatory authority for any processing of personal data by federal authorities, individuals and legal entities. The FDPIC is appointed by the Federal Council for a term of office of four years. The FDPIC supervises compliance with the DPA and other federal data protection legislation by federal bodies, and advises private bodies.

The respective Cantonal Data Protection and Information Officer in each canton is the responsible authority if personal data is processed by public authorities of the respective canton.

For breaches of marketing and unfair competition law in the use of personal data in Switzerland, claims can be filed with the State Secretariat for Economic Affairs (SECO), provided that the infringement concerns the interests of a plurality of persons (Article 10 paragraph 3 of the Unfair Competition Act). The consumers' organisations also have active legitimation in this context. In addition, the FDPIC regularly issues guidelines on data protection aspects of marketing practices. Finally, Article 45a of the Swiss Telecommunication Act foresees that providers of telecommunications services shall combat unfair mass advertising.

1.3 Administration and Enforcement Process

The FDPIC, on his or her own initiative or at the request of a third party, can investigate suspected infringements of data protection rules and request the production of files, obtain information and arrange for processed data to be disclosed to him or her.

If the investigation reveals that the DPA and its rules are being breached by federal bodies, the FDPIC can recommend that the federal body concerned changes the method of processing or abandon that processing. The FDPIC informs the department concerned or the Federal Chancellery of its recommendation. If a recommendation is not complied with or is rejected by the concerned federal body, the FDPIC may refer the matter to the department or to the Federal Chancellery for a decision. The decision is communicated to the data subjects in the form of a ruling.

If the FDPIC reveals in an investigation that, in the private sector, a natural/legal person does not comply with the DPA, it may render recommendations as well. Upon 30 days from the receipt of the recommendation, the natural/legal person must inform the FDPIC on whether it accepts and implements the recommendation or whether it rejects it. In the case of a rejection, the FDPIC may bring the case to the Swiss Federal Administrative Court. The court's decision will be binding for the parties, subject to appeal to the Federal Supreme Court. If the natural/legal person accepts the recommendation, the civil judge is not bound by this decision and can freely review it if a data subject contests said processing.

The FDPIC can also issue guidelines regarding specific processing activities. These guidelines are not binding for the judge. The FDPIC cannot start any civil proceedings for damage recovery owing to a data protection infringement.

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, such as rights to refuse to testify.

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 DPA.

In March 2019, the Schengen Federal Data Protection Act entered into force. Since Switzerland is not a member of the EU, it does not have to comply with the EU General Data Protection Regulation or any other directives applicable in this field. However, GDPR may become applicable to Swiss data processors and data controllers as long as the personal data of EU residents is concerned.

The current revision of the DPA largely aligns with the GDPR and while there is no final draft to date, it is expected that the revised DPA will be compatible with the GDPR, such that a company that complies with the GDPR should generally be in compliance with the revised DPA. Moreover, it is expected that the European Commission will continue to 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 under the Schengen agreement, Switzerland transposed, with validity as of 30 January 2019, the EU Directive 2016/680 into domestic Swiss legislation through a partial revision of the DPA.

1.5 Major NGOs and Self-Regulatory Organisations

The DPA itself does not provide an official role for NGOs and self regulated organisation (SROs). In particular, it does not grant to them active legitimation to start legal proceedings.

However, there are a number of organisations that promote privacy, including several consumer protection organisations. Furthermore, NGOs and SROs may request that the FDPIC

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 is based on the same legal principles of European data protection legislation of good faith and/or consent for any processing activity. However, there are some differences.

Under the DPA, processing by private companies does not require legal grounds, as long as the fundamental processing principles (legality, good faith, transparency, purpose limitation, proportionality, correctness and data security) are complied with. In the event of a breach of these principles, however, processing remains lawful if it is justified by the consent of the injured party, by an overriding private or public interest or by law.

The DPA protects information pertaining to legal entities much in the same way as 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.

The FDPIC has no direct enforcement powers against private bodies and individuals processing personal data.

There is no risk of criminal sanctions for a breach of data protection laws, except in very limited cases and there are no penalties for security breaches in the DPA. If the security breach also represents a breach of an obligation of secrecy, other legislation may be applicable and penalties may apply. There is a risk of civil liability towards the concerned data subjects and, depending on the circumstances, a risk of negative publicity.

1.7 Key Developments

The main developments over the past 12 months have concerned the ongoing revision of the DPA. Currently, the revision is still being discussed before the Swiss Parliament. It is expected that the final text of the revised DPA will be in line with the GDPR and be considered to grant equivalent data protection.

In the field of social insurance, legal rules were adopted in 2019 allowing social insurance providers to monitor, under certain conditions, insurance claimants in cases of suspected insurance fraud. These rules, although they entail the processing of personal data and may result in a breach of privacy rights, were justified by overriding public health interests and entered into force in October 2019.

1.8 Significant Pending Changes, Hot Topics and Issues

The finalisation of the revision of the DPA is the most significant topic in the Swiss data privacy area and everyone is awaiting the result of the last discussions before Parliament.

In addition, the Supreme Federal Court issued decisions linked with the use of dashcam recordings to report traffic offences to the police. The admission of the recordings captured by dashcams as evidence remains excluded, except in very limited cases (decision Supreme Court 6B_1188/2018).

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The key principle under the DPA is to comply with the general principles it has established – ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security (Article 4 DPA). Some of these principles are specified in more detail in specific provisions of the DPA and its Ordinance (ODPA), for example, the data security requirements.

The DPA imposes limited governance obligations (such as appointment of a data protection or privacy officer, obligation to register the files or to notify any breaches) on private entities.

The appointment of an internal data protection or privacy officer (DPO) remains optional. His or her duties are described in the ODPA. The appointment of a DPO releases the company from the obligation to notify the FDPIC of data files and of the regular processing of sensitive personal data or personality profiles or of the regular disclosure or personal data to third parties (Article 11a DPA).

Compliance with general principles of legality, good faith, transparency, purpose limitation, proportionality, correctness and data security generally suffices for the collection and other processing of personal data. In the case of a breach of these principles, however, processing is lawful only if it is justified by the consent of the injured party, by an overriding private or public interest or by law (Article 12 DPA).

There are currently no specific privacy by design and privacy by default obligations under the DPA. However, such obligations may arise under the principles 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 before processing any data. However, such obligation may arise under the principle of pro-

portionality and are usually part of the duties of an internal DPO.

There is no express requirement to adopt group or intragroup privacy policies. However, privacy notices (privacy statements) are usually adopted as contractual provisions where the processing of personal data is not reasonably to be expected by the data subjects or consent is needed for specific data processing activities, whenever sensitive personal data or personality profiles are collected.

Any person may request information from the controller of the data files as to whether data concerning him or her is being processed (right of information, Article 8 DPA). The information should be provided in writing, in the form of a printout or a photocopy, and is free of charge. The controller of a data file may refuse, restrict or defer the provision of information where a formal enactment so provides or this is required to protect the overriding interests of third parties (Article 9 DPA). The right of information cannot be waived in advance.

Any data subject may request that incorrect data be corrected. The right to be forgotten is not explicitly mentioned in the DPA, but the FDPIC and case law consider that such a right results from the general principle of proportionality and from the obligation to ensure that the data collected is correct (Article 5 DPA). Data subjects may request that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed (see Article 15 paragraph 1 DPA). It is important to note that, upon the request of the data subjects, data processing may be blocked by preliminary injunctions. There is no right to data portability set out in the DPA.

The DPA and the ODPA do not define the concept of "pseudonymous" or "anonymous" data. Generally speaking, anonymous data is data that no longer relates to an identified or identifiable person. Processing of anonymous data does not fall under the DPA. However, the act of anonymising personal data implies data processing and is therefore subject to the rules set out in the DPA. Pseudonymous data is data for which the relation to a natural or legal person is not entirely removed, but rather replaced by a code, which can be attributed based on a specific rule to the respective natural or legal person.

The DPA defines "personality profiles", as a collection of data that permits an assessment of essential characteristics of the personality of a natural person. The DPA contains a number of provisions establishing more restrictive rules for these data categories: (i) data subjects must be actively informed that sensitive data/personality profiles will be collected; (ii) disclosure of sensitive data or personality profiles to a third party (excluding processors) requires consent or another justification; and (iii) 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.

The DPA 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 are quantifiable financial damages.

2.2 Sectoral and Special Issues

The DPA defines sensitive data as data on: (i) religious, ideological, political or trade union related views or activities; (ii) health, the intimate sphere or racial origin; (iii) social security measures; and (iv) administrative or criminal proceedings and sanctions. The personality profile benefits from the same protection as sensitive data (Article 3 litterae c and d DPA).

Financial Data

Several laws in the financial sector contain provisions on dealing with data. Under the Banking Act (Article 47), it is a criminal offence for an employee, agent or representative of a bank to disclose any information confided to them, or of which they become aware, 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. However, financial data itself is not considered to be personal data in the sense of the DPA.

Health Data

Data on health-related issues is statutorily defined as sensitive personal data, to which stricter rules apply (Article 3 c DPA). These stricter rules require the data controller to inform the person about the collection of sensitive personal data. The disclosure of sensitive data to third parties is possible only with express consent, by an overriding public or private interest or by law (Article 12 DPA). Data files containing health data need to be notified and registered with the FDPIC (Article 11 DPA)

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 in respect of the medical and health data

of their patients. An infringement of such obligations may be prosecuted 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 limitations on use of personal data under the DPA. Disclosing information relating to subscribers' communications to a third party without consent amounts to a criminal offence.

Children's Data
The personal data of children and adults is protected in the same way under the FDPA. 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. The general provisions of the DPA will apply to such data, and cantonal privacy laws apply to cantonal and communal authorities, including public schools dealing with such data.

Internet, Streaming and Video
There are no laws specifically targeting the processing of personal data on or by social media, search engines and online platforms. The liability of online platform providers and intermediaries when the privacy of their users is infringed by third parties is not fully clear and is judged on a case-by-case basis. As a general rule, providers are 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 that content.

Browsing data
There are no laws specifically targeting browsing and viewing data containing personal data. However, the processing of such data must comply with the general principles in respect of the processing of any personal data – ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security.

Cookies
Swiss law does not require an explicit opt-in regarding cookies. Accordingly, it is sufficient to inform the website users about cookies, the data processed by cookies, the purpose of that processing and opt-out mechanisms (see Article 45c of the Swiss Telecommunication Act). Failure to provide the required information may lead to a fine of up to CHF5,000.

Location data
There are no laws specifically targeting geolocation data. However, processing of such data must comply with the general principles in respect of the processing of any personal data – ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security.

Do not track
There is no obligation for software providers to include or activate by default a "do-not-track" option.

Behavioural advertising
The processing of personal data is generally lawful if it is in accordance with the legal principles set forth in the DPA. As a general rule, behavioural advertising is permitted without consent if the data subjects are notified about the existence of such advertising and its content in a privacy notice made available in advance. Such notification may also include the fact that behavioural advertising may include sensitive personal data, such as personality profiles. In any case, restrictions and requirements under the FTA, as well as under the Unfair Competition Act, as regards electronic mass advertisements must be complied with when using cookies to shape advertising to based on the data subject's behaviour.

Social media and search engines
There is no legislation specifically targeting technologies such as social media, search engines and online platforms. The key regulations in this respect are included in the DPA 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 the obligation to prevent infringements of privacy, online platform providers and intermediaries are generally not obliged to monitor their traffic for illegal content and may not become liable for such content, but if they are notified of illegal content by a judicial order they are under an obligation to block access to or remove that content.

Hate speech
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 (Article 261bis Criminal Code).

Other Issues
Right to be forgotten
Any data subject may request that incorrect data be deleted (see Article 5 paragraph 2 DPA). The right to be forgotten is not explicitly mentioned in the DPA, but the FDPIC and case law consider that such a right may result from the general principle of proportionality. Thus, a the data subject may ask for, and

receive, erasure if no statutory retention obligation or prevailing Swiss public or private interest overrides the request.

Data access and portability

Any person may request information from the controller of the data file as to whether data concerning him or her is being processed. The information must normally be provided in writing, in the form of a printout or a photocopy, and be free of charge (Article 8 DPA). However, there is no right of portability set out in the DPA.

Right of rectification or correction

Any data subject may request that incorrect data be corrected (see Article 5 paragraph 2 DPA).

2.3 Online Marketing

With regard to marketing communications distributed by telephone, email or fax, Article 3 littera u Unfair Competition Act prohibits the sending of such communication if the recipient has declared in the official telephone registry that he or she does not wish to receive such communication.

Regarding mass emails and text messages, Article 3 littera o Unfair Competition Act requires that such communication is only sent with the prior consent of the recipients (opt-in) and with clear information on a simple opt-out procedure. An exception is made if the entity received the contact information in connection with the sale of products or services and if the customer was informed at the moment of the data collection about the simple opt-out procedure. In that case, information regarding similar products or services may be sent without prior consent.

Article 3 littera u Unfair Competition Act prohibits marketing communication via telephone, email and fax if the recipient has declared in any telephone registry that he or she does not wish to receive such communication. In addition, there are several industry-related "do not contact" lists (such as codes of conduct), which many companies respect but which are not mandatory.

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

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

2.4 Workplace Privacy

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 not 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 at their working place, except if those monitoring systems are necessary for other legitimate reasons, such as security, and do not negatively affect the health and mobility of employees.

The FDPIC has issued specific guidelines on the processing of employee data, which Swiss employers are recommended to follow.

Monitoring of Workplace Communications

In accordance with the DPA and Article 328b of the Swiss Code of Obligation, the employee must be informed, transparently and in advance, about the type and method of the electronic monitoring, the scope and period of the monitoring, and its purpose.

Anonymous monitoring (including monitoring of search strings) of, for example, employees' use of company-provided information technology, according to email and internet user guides or other policies, is permissible. Pseudonymous monitoring (ie, the monitoring of an employee known only to a very limited group of persons) is only permissible for spot checks. No continuous monitoring is permissible in this case.

In both cases, the employees must be informed of the fact that their information technology use can/will be monitored. They may be informed through monitoring policies made available in advance.

Systematic and permanent monitoring of the information technology use of specific employees is not permitted, unless:

- the employee has freely consented thereto, provided that he or she has been transparently informed of the monitoring and it is proportional to its purpose; or
- if there is no consent, then the following requirements have been fulfilled:
  - (a) justified suspicion of a criminal offence;
  - (b) monitoring and reading of emails is necessary to confirm or dispel suspicion;
  - (c) conserving of evidence; and
  - (d) there is no overriding interest of the employee.

If there is an overriding interest, then the consent of the employee must be obtained. Please note that any evidence not collected in compliance with the applicable law may not be admissible in court.

Accordingly, the use of so-called spyware, which clandestinely monitors the conduct of a specific employee in the workplace (eg, computer screen movements), is not permitted and would infringe Swiss law. According to the FDPIC, this also applies to so-called content scanners (if done clandestinely). A content scanner is software that evaluates/scans sent and received emails in accordance with predefined keywords and reacts accordingly (cancellation or blocking of emails, etc).

Clandestine and not pre-announced monitoring is prohibited and cannot be justified by an overriding interest of the employer. Finally, there are also specific provisions concerning the monitoring of employees in the labour laws.

Labour Organisations

The representatives of the employees in a company have a right to timely and comprehensive information from the employer on all matters that allow employees to duly perform their tasks (Article 9 of the Federal Act on Information and Participation of Employees in Companies). Since employee monitoring may have an impact on employee performance, employee representatives need to be kept up to date on this subject. However, there is no requirement to consult any entities.

Whistle-Blowing

There is currently no specific legislation, nor any provisions, under Swiss law on whistle-blowing, as such. There are ongoing attempts to regulate whistle-blowing and to provide protection for whistle-blowers. Currently, the protection of the employee as a whistle-blower is very weak. The employee is potentially exposed to sanctions that are both civil (eg, termination of his or her job, potential damages) and criminal (eg, offences due to false allegations, industrial espionage and infringement of blocking statutes if the allegations are reported abroad, see below). There are no restrictions, as such, as to what can be reported to a whistle-blower hotline.

Moreover, there is no duty to notify or register the whistle-blower hotline with the respective authorities. However, collections of sensitive personal data or personality profiles must be registered with the FDPIC, even if the persons concerned are aware of the processing (Article 11 DPA). However, if whistle-blower hotlines collect employees' personal data and regularly disclose them to third parties, there is a duty to register. Excluded from this is data collections by companies which have appointed an internal Data Protection Officer. Swiss doctrine is mainly of the opinion that companies with whistle-blower hotlines do not have to register their respective data collection, because there is usually no sensitive personal data or employee personality profiles among that data and, even if there was such sensitive personal data, it is not processed on a regular basis.

Whistle-blowing is mainly discussed in Switzerland in connection with the loyalty and confidentiality duties of the employee, the provisions regarding justified termination, and the employer's duty of care towards its employees. The employer must implement all necessary measures in order to ensure that the personality rights of the whistle-blower are not infringed (Article 328 Code of Obligations). Accordingly, the employee must be informed transparently and comprehensively about all aspects of the whistle-blower hotline (where it is operated, who is operating it, etc) and of the consequences his or her whistle-blowing activities may have before using the hotline.

There are no provisions prohibiting or discouraging anonymous reporting. In practice, it is, however, often recommended not to report anonymously. The main argument in favour of non-anonymous reports is the transparency principle in Article 4 paragraph 4 DPA. An employee suspected of misconduct in a whistle-blowing report must be informed about the report, the whistle-blower and the alleged misconduct. It is acceptable to delay informing the suspected employee in order to facilitate investigations.

Issues of e-Discovery

Much depends on whether requests are made during pending proceedings or outside of such proceedings.

During pending proceedings, the companies are not permitted to (directly) respond to such requests. The foreign law enforcement agency must contact the competent Swiss authorities within the international judicial assistance (in civil or criminal matters) system. The Swiss authority then collects and transfers the respective information by way of judicial assistance to the foreign authority. The DPA is not applicable in the case of judicial assistance proceedings (see Article 2 paragraph 2 littera c DPA).

The so-called Swiss blocking statutes (eg, Articles 271 and 273 of the Swiss Criminal Code) are most relevant in this context. Due to the blocking statutes, companies within Switzerland that are not voluntary party to a foreign procedure cannot comply with foreign e-discovery requests without incurring the risk of a penal prosecution for unpermitted disclosure. It must be decided on a case-by-case basis whether such requests can be complied with or whether a specific waiver from the competent authorities must be obtained (if applicable). If a Swiss company violates the blocking statutes, its board members might be considered as responsible persons and sanctioned with a fine or imprisonment.

2.5 Enforcement and Litigation

Potential Enforcement Penalties

The FDPIC cannot open an investigation unless a suspected privacy breach is capable of affecting a large number of persons (system error) and in limited additional cases (Article 29 DPA). The FDPIC has no right to impose criminal and/or administrative sanctions itself.

The FDPIC can issue recommendations regarding the set-up of specific processing activities. These may include the recommendation to abandon certain processing activities or to amend a processing activity. If the party concerned does not follow the issued recommendations or rejects them, the FDPIC may involve the Administrative Federal Court. The court's decision will be binding for the parties, subject to appeal to the Federal Supreme Court. If the Federal Administrative Court issues a binding order, it may impose fines for non-compliance with that order.

There is a risk of criminal fines issued by the criminal courts in very limited cases, for example when there is a breach of obligations to provide information, to register data files or to co-operate (Article 34 DPA) and/or a breach of professional confidentiality – eg, by attorneys at law or physicians (Article 35 DPA).

Private Litigation

A breach of privacy and data protection rules may give rise to civil cease-and-desist claims and claims for damage compensation. Allegations of a breach of privacy are often a support to contractual claims as well, for example, in employment litigation.

Class actions are currently not allowed in Switzerland

Leading Enforcement Cases

The Swiss Federal Supreme Court has dealt with the implementation of video surveillance by the police (Decision 6B_181/2018 of 20 December 2018). The Swiss Federal Supreme Court ruled that such surveillance is a coercive measure that should be ordered by the prosecution with the approval of the specific court responsible for monitoring coercive measures only. The employer's agreement to monitor its employees suspected of theft does not constitute consent to the implementation of such a measure. Once the police have installed the video surveillance without respecting these legal requirements, the information collected cannot be used as evidence and must be destroyed.

The Swiss Supreme Court also ruled in a recent decision (Decision 6B_91/2018 of 27 December 2018) with regard to the exchange of personal data collected during criminal proceedings. The Swiss Federal Supreme Court confirmed the lower court's decision, according to which the criminal justice authority may disclose personal data from pending proceedings for use in other criminal, civil or administrative pending proceedings provided that the data may provide essential information and is not contrary to any overriding public or private interests, according to Article 96 and Article 101 paragraph 2 of the Swiss Criminal Procedure Code. In the case at hand, the Attorney General issued, during a criminal investigation, a freezing order on the sum of CHF7,000, which the accused had won at the casino two days prior to the attachment. Since the Attorney General was aware that the accused was subject to several certificates of shortfall, it decided to inform the debt collection office of the seized assets. Upon the debt collection office's request, the Attorney General then transferred the seized assets in order for them to be part of the attachment proceedings.

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 most relevant legal bases which law enforcement, prosecution authorities and national security and intelligences services rely on for surveillance purposes.

Surveillance measures, surveillance in public places, and information requests (eg, about telecommunications services user identity) do not necessarily require prior approval of judicial authorities, but can rely on the authority given by the legal provisions. More intrusive measures, typically live surveillance and communications interception, do, however, require judicial approval. That being said, in many cases surveillance measures can be carried out secretly, without the data subject's (immediate) knowledge.

Personal data is protected by civil, administrative and penal procedural rules. A cross-border data transfer for the prevention, investigation and prosecution of criminal acts is only permitted if the privacy is protected by international agreements. Most relevant for Switzerland is the implementation of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in force through the amendment of the DPA and other legal provisions since 1 March 2019.

Under Swiss law, data protection essentially applies regardless of the seriousness of the crimes concerned.

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

See **3.1 Laws and Standards for Access to Data for Serious Crimes**.

3.3 Invoking a Foreign Government

In the absence of an order issued by the competent Swiss court, requests from foreign governments do not allow for the collection and transfer of personal data located in Switzerland. To the contrary, any disclosure of documents and personal data to foreign authorities or agencies will result in a breach of the penal blocking statutes, legal provisions forbidding any investigation or other sovereign activities of foreign governments on the Swiss territory (Article 271 Penal Code).

Switzerland does not participate in a Cloud Act agreement with the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

There are no issues that arises in our jurisdiction with respect to national security access and surveillance because each surveillance measure is, in principle, under the supervision of a judge.

4. International Considerations

4.1 Restrictions on International Data Issues

International or cross-border disclosure includes any transfer of personal data abroad, including allowing examination (eg, of an online database), transfer or publication (see Article 3 littera f DPA). Personal data must not be disclosed abroad if the personal integrity of those concerned would thereby be seriously harmed (see Article 6 paragraph 1 DPA). A serious violation of personal integrity is assumed if there is no legislation ensuring an adequate level of protection in the country where the data is disclosed. The FDPIC maintains a list of countries that ensure an adequate level of data protection. With regard to personal data related to individuals, all EU and EEA member states are considered to provide an adequate level of data protection.

The conditions covering disclosure of data abroad are applicable irrespective of whether the transfer takes place within the same corporate body or to another legal entity.

4.2 Mechanisms That Apply to International Data Transfers

The assumption that privacy rights are violated by a disclosure of personal data to a country without appropriate data protection laws can only be refuted if at least one of the minimum conditions stipulated in Article 6 paragraph 2 litterae a to g DPA is present. However, the possibility of justifying the admissibility of the international data transfer based on the general grounds for justification (according to Article 13 DPA) is not available.

As a rule of thumb, all countries which have either ratified the ETS 108 agreement or are subject to the EU's GDPR are considered to have an adequate level of data protection according to Swiss legislation.

In addition, the FDPIC has prepared a non-binding list of those countries whose data protection legislation should ensure appropriate protection. However, additional precautions according to Article 6 paragraph 2 DPA may be advisable.

The transfer of data abroad within a group of companies is also permissible to countries without an adequate level of data protection if the companies concerned are subject to group-wide data protection rules which ensure appropriate protection. This regulation privileges international data transfers within a group of companies (Article 6 paragraph 2 littera g DPA).

Data protection rules which ensure adequate protection must at least contain the elements recommended by the FDPIC for international data transfers; namely:

- list of purposes of use, split up according to categories of personal data;
- binding agreement on disclosing data for indicated purposes only;
- protection of the rights of the persons concerned (in particular, rights to information and correction);
- ban on transfer of data to a third party;
- ensuring data security in accordance with the sensitivity of the data; and
- stipulation of compensation liability of the data recipient for violation of contract.

If there are both inadequate legislation in the recipient country and insufficient data protection rules within the company, international data transfers among affiliated companies in the group are still permitted, provided one of the minimum requirements of Article 6 paragraph 2 litterae a to f DPA is satisfied:

- sufficient safeguards, in particular contractual clauses, to ensure an adequate level of protection abroad;
- the data subject has consented in the specific case;
- the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;

- disclosure is essential in the specific case in order to either safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject; or
- the data subject has made the data generally accessible and has not expressly prohibited its processing.

Most legal entities use the EU standard contractual clauses as sufficient safeguards in the sense of Article 6 paragraph 2 littera a DPA. The use of the EU standard contractual clauses also facilitates the notification of the cross-border transfer to the FDPIC (see **4.3 Government Notifications and Approvals**). Also, a transfer of personal data under the framework of the US/Switzerland Privacy Shield is considered to grant adequate data protection.

4.3 Government Notifications and Approvals

There is no general requirement to register or notify, or apply for approval. The FDPIC has to be notified only in two instances: the FDPIC has to be informed of the fact that adequate contractual guarantees (Article 6 paragraph 2 littera a DPA) have been concluded or that data protection rules within the group of companies (Article 6 paragraph 2 littera g DPA) have been implemented. As long as the contractual guarantees are in line with the provisions in the EU standard contractual clauses, the respective data protection agreement does not have to be submitted. The group internal rules also need to be submitted to the FDPIC (Article 6 paragraph 3 DPA and Article 6 paragraph 5 ODPA). In both instances, it suffices to inform the FDPIC of the existence of such rules and guarantees. The FDPIC can nevertheless start a data protection compliance review on its own.

The FDPIC must be informed about these safeguards prior to cross-border disclosure (see Article 6 paragraph 3 DPA and Article 6 paragraph 1 ODPA).

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. Some codes of conduct, such as the one for Swiss physicians, also recommend storage of personal data of patients in Switzerland – ie, on Swiss based clouds.

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

So-called 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 mandatory instruction of a foreign authority or is made in accordance with rules on international judicial assistance.

4.7 "Blocking" Statutes

In addition to Article 271 of the Criminal Code, noted in **4.6 Limitations and Considerations**, 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 Aricle. 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 are no laws specifically targeting big data and related analytics. However, should the data not be fully anonymised or pseudonomised, its processing must comply with the general principles of data protection – ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security.

There are no laws specifically targeting automated decision-making, artificial intelligence (including machine learning), the Internet of Things (IoT), autonomous decision-making (including autonomous vehicles) or biometric data. However, the processing of such data must comply with the general principles of data protection – ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security.

The DPA contains specific rules concerning "personality profile" which are protected like sensitive date (Article 3 DPA)

There are no laws specifically targeting facial recognition. Such data is considered to be sensitive data and specific restrictions

apply based on the DPA. In addition, processing of such data must comply with the general principles of data protection.

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 DPA. As this ruling was rendered in a specific situation, 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.

In the revised DPA, biometric data will be considered sensitive personal data and protected accordingly.

There are no laws specifically targeting geolocation. However, the processing of such data, as soon as it permits the identification of an individual, must comply with the general principles of data protection.

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.

5.2 "Digital Governance" or Fair Data Practice Review Boards

There are no organisations establishing protocols for digital governance or fair data practice review boards or committees in Switzerland. However, some organisations are issuing rules in their specific field of activity.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

The sanctions under the DPA are limited as well as the investigative possibilities available to the FDPIC. Therefore there are no significant audits, investigations or penalties imposed in cases of data protection violation. Recommendations in this respect are regularly issued by the FDPIC.

Class actions, forms of collective redress or representative actions are currently not available under Swiss procedural rules.

5.4 Due Diligence

In the case of due diligence, companies are required to comply with the general principles of data protection – ie, legality, good faith, transparency, purpose limitation, proportionality, correctness and data security.

There are typically two main areas of risk with regard to data protection breaches during the due diligence process: the unlawful processing and the unlawful transfer of data. During the preparation and conclusion of the contract, the company may transfer too much personal data as part of the due diligence process (violation of the principle of proportionality and no overriding private interest), and potential buyers may obtain information (eg, about individuals) that they do not need in order to decide to take over the company. In the takeover phase, there is a risk that personal data may used for a purpose other than that stated at the time of collection.

In respect of any due diligence, it is imperative to assess and take in to consideration any potential data protection risks.

5.5 Public Disclosure

Currently, there are no obligations to disclosure cybersecurity risk profiles. Also, data breaches are not subject to specific notification or reporting obligations to the regulatory authorities, although proper data security practices under the DPA and DPO (as well as sectorial regulations), combined with the general principle of transparency, may of course lead to (the need for) breach notifications to the concerned data subjects.

The legal framework is expected to change under the revised DPA as it is a matter of compliance by Switzerland with the requirements of the revised Council of Europe's Convention 108.

5.6 Other Significant Issues

There are no significant issues in data protection and privacy in Switzerland not already addressed in this chapter.

Pestalozzi is a multicultural Swiss business law firm that has focused on high-end work for domestic and international clients since 1911. Pestalozzi lawyers are strong and empathic personalities who are singled out by the truly independent approach taken in their advice and representation of their clients' interests. The firm guides and supports its clients in their strategic business decisions, anticipates their future challenges and helps them solve their critical issues. Being fully integrated, Pestalozzi encounters no internal limits in shaping the most adequate and efficient teams for its clients' needs. With over 100 professionals in Zurich and Geneva, they are at home in Switzerland's two main commercial hubs – and have developed a wealth of experience in their key industries of banking, life sciences, commodity trading and insurance. While being locally embedded, it has also developed a sought-after expertise in dealing with multi-jurisdictional transactions and disputes.

Authors

Lorenza Ferrari Hofer is head of Pestalozzi's IP&TMT group and co-head of the life sciences group. She specialises in intellectual property, unfair competition, data law, data protection and contract law. Lorenza Ferrari Hofer has years of experience in structuring complex R&D, know-how transfer and co-operation projects, particularly in the field of life sciences. She assists technology corporations as well as research institutions in both negotiations and strategic matters, and represents them in legal proceedings in Swiss courts, arbitral tribunals and regulatory authorities. In addition, she has a broad knowledge of media, advertising and entertainment matters, where she regularly represents and advises companies and individuals in respect of copyright, unfair competition and privacy law issues.

Michèle Burnier is a partner of Pestalozzi's IP&TMT group in Geneva. Her fields of expertise include intellectual property, including geographical indications, TRIPS Agreement, unfair competition, data protection, advertising and e-commerce law, IT and telecommunications as well as administrative and contract law. She regularly represents clients before Swiss civil or criminal courts in relation to her IP&TMT practice. She has years of experience in negotiating and drafting of complex IP agreements. Furthermore, she frequently acts as arbitral secretary under the ICC Rules or Swiss Rules.

Pestalozzi Attorneys at Law Ltd

Loewenstrasse 1
8001 Zurich
Switzerland

Tel: +41 44 217 91 11
Fax: +41 44 217 92 17
Email: zrh@pestalozzilaw.com
Web: www.pestalozzilaw.com