COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Switzerland

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

Pestalozzi

Michèle Burnier

Partner | michele.burnier@pestalozzilaw.com

This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in Switzerland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

SWITZERLAND
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

The following answers are based on the current legal and regulatory framework. It should be noted, however, that the Federal Act on Data Protection of 19 June 1992 (DPA) and the Ordinance to the Federal Act on Data Protection of 14 June 1993 (ODPA), which are the most important laws in the field of data protection in Switzerland, are currently being revised. The referendum deadline against the revised DPA expired unused at the beginning of 2021. It is expected to come into force in September 2023. The main purpose of the revision is to align the DPA's standard of protection with the standard of protection offered by the EU General Data Protection Regulation (GDPR). This said, however, the provisions of the GDPR will not simply be copied. There will remain differences.

In Switzerland, data protection is regulated on the federal and cantonal level. On a federal level, the Swiss Constitution of 18 April 1999 (SC) protects the right to privacy, in particular the right to be protected against the misuse of personal data (Article 13 SC). The DPA and the ODPA regulate the processing of personal data by natural and legal private persons and federal bodies. In addition, every Swiss canton has its own data protection statutes with respect to data processing by cantonal bodies (including the communes).

There are various laws containing additional, sector-specific regulations on privacy. For instance, in the fields of labor law, healthcare insurance, human research, banking and finance, telecommunication or related to unfair competition.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

The DPA provides for an obligation to register data files for the controller of such data files (Article 11a DPA). A "data file" is any set of personal data that is structured in such a way that the data is accessible by data subject (Article 3 lit. g DPA). "Controller of the data file" is the private person or federal body that decides on the purpose and content of the data file (Article 3 lit. i DPA).

Federal bodies must declare all their data files to the Federal Data Protection and Information Commissioner (FDPIC; Article 11a para. 2 DPA). Private persons must declare their data sets to the FDPIC if (i) they regularly process sensitive personal data or personality pro-files; or (ii) they regularly disclose personal data to third parties (Article 11a para. 3 DPA; for definitions see Question 3).

Article 11a para. 5 DPA and Article 4 ODPA provide for several exemptions. For example, a controller must not declare his files if, for example, private persons process data in terms of a statutory obligation (Article 11a para. 5 lit. a DPA), or the controller has designated a data protection officer (DPO; Article 11a para. 5 lit. e DPA). Please note that this obligation to register will be abolished with the entry into force of the new DPA.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII?

What other key definitions are set forth in the laws in your jurisdiction?

“Personal data” are all information relating to an identified or identifiable natural or legal person (Article 3 lit. a in conjunction with Article 3 lit. b DPA). According to case law (see BGE 136 II 508, c. 3.2), “a person is identified when it is clear from the information itself that it is exactly this person. The person is identifiable if he or she can be inferred from additional information. However, not every theoretical possibility of identification is sufficient for identifiability. If the effort is so great that, according to general life experience, it is not to be expected that an interested party will take it upon himself, there is no identifiability. The question is to be answered depending on the concrete case, whereby in particular also the possibilities provided by technology are to be considered, so for example the search tools available on the Internet. Of importance, however, is not only what effort is objectively required to be able to assign a certain piece of information to a person, but also what interest the data processor or a third party has in identification.”

“Sensitive personal data” are data on (i) religious, ideological, political or trade union-related views or activities, (ii) health, the intimate sphere or the racial origin, (iii) social security measures, and (iv) administrative or criminal proceedings and sanctions (Article 3 lit. c DPA).

“Personality profile” means a collection of data that permits an assessment of essential characteristics of the personality of a natural person (Article 3 lit. d DPA). This category of data benefits from the same protection as sensitive data

“Processing” means any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data (Article 3 lit. e DPA).

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or “fair information practice principles” in detail.

Federal bodies may only process personal data if such processing is explicitly justified by law (Article 17 para. 1 DPA).

On the other hand, the processing of personal data by private persons does in general not require legal basis, as long as the general data processing principles are complied with (Article 12 para. 2 lit. a DPA e contrario). The general principles of data processing are the following:

- Principle of legality (Article 4 para. 1 DPA): The processing of personal data has to comply with Swiss law.
- Principle of good faith and proportionality (Article 4 para. 2 DPA): Personal data may only be processed, if such processing is necessary and appropriate to achieve a legitimate purpose. Further, one may process only as little data and for as long as necessary for pursuing the purpose intended.
- Principle of transparency (Article 4 para. 2 and 4 in conjunction with art. 7a DPA): The collection of personal data and in particular the purpose of its processing must be evident to the data subject. Active and comprehensive information is only required if (i) the processing and/or its purpose is not evident to the data subject, or (ii) sensitive personal data or personality profiles are processed (Article 14 DPA); this duty to provide information also applies where the data is collected from third parties.
- Principle of purpose limitation (Article 4 para. 3 DPA): Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.
- Principle of data accuracy (Article 5 para. 1 DPA): Personal data must be accurate and up to date. Personal data that is incorrect, incomplete, or no longer required in view of the purpose of its collection is either to be corrected or destroyed.
- Principle of data security (Article 7 para. 1 DPA): Personal data must be protected against any unlawful processing by appropriate organizational and technical measures.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

In general, the processing of personal data does not

require justification, such as the consent of the data subject, if the principles of data processing are respected (see Question 4).

The processing of personal data in violation of the processing principles is considered a breach of personality rights of the data subject concerned. Such breach of personality rights is deemed unlawful unless it can be justified by the consent of the data subject, an overriding private or public interest, or a statutory provision of Swiss law (Article 13 para. 1 DPA).

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information before the processing (Article 4 para. 5 DPA). Such information must include, for example, what kind of personal data is collected, for what purpose and by what means, and whether the collected personal data is disclosed and transferred to third parties in countries, where there is no adequate data protection.

If sensitive personal data and/or personality profiles are processed, the data subject must expressly consent in such processing (Article 4 para. 5 DPA). Consent is given expressly when the data subject's consent is expressed directly, for example, by confirming a declaration of consent by clicking a checkbox.

In principle, consent is not valid if it is given while there is a relationship of subordination or dependence with the data controller. Finally, the consent can be revoked at any time.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

When processing sensitive personal data or personality profiles, the data controller must provide active and comprehensive information to the data subject (Article 14 DPA). Further, the disclosure of sensitive personal data or personality profiles to third parties must be justified, either by the explicit consent of the data subject, an overriding private or public interest, or a statutory provision of Swiss law (Article 12 para. 2 lit. c DPA).

Private persons must declare their data files if they regularly process sensitive personal data or personality profiles (Article 11a para. 3 DPA), unless an exception under Article 11a para. 5 DPA applies.

Under the DPA, there are no categories of personal data that are prohibited from processing.

8. How do the laws in your jurisdiction address children's personal data or PII?

The DPA does not provide for special or different regulations regarding the processing of personal data of children.

When the consent is required and depending on the processing, the consent of the legal representatives must be obtained.

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

According to Article 2 para. 2 DPA, the DPA does not apply to (i) personal data that is processed by a natural person exclusively for personal use and which is not disclosed to outsiders, (ii) deliberations of the Federal Assembly and in parliamentary committees, (iii) pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance, (iv) public registers based on private law, and (v) personal data processed by the International Committee of the Red Cross.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

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.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

There are currently no specific obligations under the DPA to maintain records of the data processing activities. However, an obligation to maintain records may result from the following reasons:

- Register of data files (Article 11a para. 5 lit. e DPA): The internal DPO, if one is appointed, must maintain a list of the data files.
- Automated processing (Article 10 ODPA): The controller of the data file must maintain a record of the automated processing of sensitive personal data or personality profiles if preventive measures cannot ensure data protection. Records are necessary in particular, if it would not otherwise be possible to determine subsequently whether data has been processed for the purposes for which it was collected or disclosed.
- Access right (Article 8 et seq. DPA): To comply with access requests, written documentation of the processing activities may be necessary. The same applies to deletion or correction requests.
- Data security (Article 7 DPA): The appropriate technical and organizational measures must be documented in writing and may include the establishment of internal processes and policies. This applies in particular to the controller of an automated data file subject to registration (Article 11a para. 3 DPA) that is not exempted from the registration requirement in terms of Article 11a para. 5 lit. b-d DPA. Such controller shall issue a processing policy that describes the internal organization and the data processing and control procedures and contain documents on the planning, realization and operation of the data file and the information technology used (Article 11 para. 1 ODPA).
- Data processing by third parties (Article 10a DPA): The processing of personal data may be assigned to third parties but the instructing party must in particular ensure that the third party guarantees data security.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

There is no requirement under the DPA to have data retention and data disposal policies and procedures.

Regarding personal data, they must be deleted as soon as they are no longer needed. The retention period must be determined individually for each data category. Before archiving all documents (electronically or paper), it is therefore necessary to first clarify if the data must be kept by law and data whose retention is in the data controller' s best interest, such as documents required to fulfil legal or mandatory contractual obligations.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

Under the DPA, consultations with the FDPIC are not required, but quite common to discuss specific data processing activities or the interpretation of particular provisions.

In case of cross border disclosure, the FDPIC must be informed of the safeguards under Article 6 para. 2 letter a DPA and the data protection rules under Article 6 para. 2 letter g DPA.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

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

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

There is no requirement to appoint a DPO. However,

DPOs are often appointed to avoid the notification of data files to the FDPIC (Article 11a para. 5 lit. e DPA).

If appointed, the responsibilities of the DPO are set out in Article 12b para. 1 ODPA. Accordingly, the DPO (i) audits the processing of personal data and recommends corrective measures if he ascertains that the data protection regulations have been infringed, and (ii) maintains a list of the data files in accordance with Article 11a para. 3 DPA that are operated by the controller of the data files; this list must be made available to the FDPIC or on request to data subjects.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

There are currently no specific obligations under the DPA to train employees. However, from a good corporate governance perspective, we would recommend that companies do so in order to minimize the risk of a breach of the DPA.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

Controllers must actively inform data subjects about the collection of personal data and the purpose of the data processing, if this information is not apparent to the data subject from the context or the particular constellation of the data processing (Article 4 para. 4 DPA). In any case, active information is necessary if sensitive personal data or personality profile is processed (Article 14 DPA).

This said, however, it is good practice to have data privacy policies in place that fully inform data subjects about data processing.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

DPA does not use the terms “controller” and “processor”. Instead, it refers to the “controller of the data file” and to the third party who processes data on behalf of another (Article 3 lit. i and 10a DPA). Although the two roles are not congruent, a largely identical understanding has been established in Switzerland with regard to “controller” and “processor”, as this is applied under the GDPR. Accordingly, a “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. “Processor” means the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

The controller is the person responsible for the legality of the data processing. No obligations are placed on the processor by operation of law. However, processors are regularly subject to contractual obligations towards the controller.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

DPA does not require any minimum contract terms and it is not even compulsory to enter into a written contract with a processor. Accordingly, there are no specific restrictions relating to the appointment of a processor. However, the controller must ensure that the provider ensures data security (Article 10a para. 2 DPA). Further, the controller remains responsible for data processing infringements by the provider. The controller will therefore have an interest in carefully selecting, instructing, and supervising the processor. Depending on the nature of the data processed (for examples, insurance, bank, etc.), special laws may impose particular requirements.

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

DPA does not define the terms “monitoring” and “profiling”. However, monitoring and profiling are

considered to be processing activities within the meaning of the DPA. If personal data is processed in these activities, the data processing principles must be respected. In addition, monitoring and profiling may, under certain circumstances, result in personality profiles. This may result in stricter requirements for data processing, e.g., the need for justification (see Question 6).

With regard to the use of cookies, Article 45c lit. b of the Telecommunications Act sets out that the processing of data on external equipment by means of transmission using telecommunications techniques is permitted only if users are informed about the processing and its purpose and are informed that they may refuse to allow processing. Against this background, the DPA does not require consent to use cookies.

In addition, depending on the direction of the website, further requirements may arise from the European E-Privacy Directive.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

DPA does not define “cross-contextual behavioral advertising”. However, DPA defines personality profile, namely a collection of data that permits an assessment of essential characteristics of the personality of a natural person. Personality profile benefits from the same protection as sensitive data.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is “sale” or related terms defined and what restrictions are imposed, if any?

Under Swiss law there is currently no law dealing specifically with the sale of personal information. However, the commercialization of personal information must comply with the rules of the DPA.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

DPA does not define “e-mail communication” or “direct marketing”. Under the DPA, the processing of e-mail addresses for marketing purposes does not require justification, as long as the general data processing principles are respected.

With respect to e-mail marketing, the DPA is superseded by the Federal Act on Unfair Competition (UCA). According to Article 3 para. 1 lit. o UCA, anyone acts unfair who sends or causes to be sent mass advertising without a direct link to a requested content by telecommunications, without first obtaining the consent of the customer, indicating the correct sender, or indicating a possibility of refusal without any problems and free of charge; anyone who receives contact information from customers when selling goods, works or services and indicates the possibility of refusal does not act unfairly if he sends mass advertising for his own similar goods, works or services to these customers without their consent.

Therefore, from an unfair competition perspective, mass advertising that is not directly related to requested content is only permissible with the prior, informed and voluntary consent of the customer (opt-in). The sender must inform the customers about their right to withdraw at any time. The customer’s consent does not have to be explicit. However, obtaining express consent is recommended for reasons of evidence. The customer’s consent is not required if mass advertising is directly related to requested content and if the sender informs the customers about their right to withdraw prior to the sending of the first marketing e-mail. It is not sufficient, if the withdrawal right is only mentioned in the marketing e-mail.

In addition and according to Article 3 para. 1 lit. s UCA, anyone acts unfair who offers goods, works or services by means of electronic commerce without: 1) indicating in a clear and complete manner their identity and contact address, including the contact details for electronic mail, 2) indicating each technical step leading to the conclusion of a contract, 3) providing the adequate technical means that allow for recognition and correction of input errors before submission of the order, and 4) confirming the client’s order immediately by electronic means.

As regards telephone calls and text messaging, anyone acts unfair who does not respect the mention in the directory stating that a client does not want to receive advertisements from third parties and that his or her data must not be shared for purposes of direct advertisement (Article 3 para. 1 lit. u UCA). In addition, it is unfair to make advertising calls without displaying a telephone number listed in the directory and for which it has a right of use (Article 3 para. 1 lit. v UCA).

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

DPA does not provide for specific regulations regarding biometrics and does not define the term. However, biometric data (e.g., voice, fingerprint, face shape) qualify as personal data. Depending on the biometric characteristics processed, these data may contain additional information about, e.g., the race or health status of the data subject. In this case, biometric data qualify as sensitive personal data, which are subject to stricter processing requirements.

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

Under Swiss law, a data transfer abroad occurs when personal data is transferred from Switzerland to a country outside Switzerland, or when personal data located in Switzerland is accessed from outside Switzerland.

Without further safeguards, personal data may be transferred only to countries providing for an adequate data protection level (Article 6 para. 1 DPA). The FDPIC has published a (non-binding) list of countries that he considers to have such an adequate level of data protection.

For data transfers to countries without an adequate data protection level, additional safeguards are required. Article 6 para. 2 DPA contains a list with acceptable safeguards such as contractual clauses ensuring an adequate level of protection abroad (e.g., amended EU standard contractual clauses), corporate binding rules, or the data subject's consent.

The controller shall inform the FDPIC if the controller intends to base his or her data transfers on contractual clauses or corporate binding rules (Article 6 para. 3 DPA). The duty to provide information is also regarded as fulfilled if data is transferred on the basis of the (unchanged) template outsourcing agreement that have been drawn up by the FDPIC, and the FDPIC has been informed about that use by the controller (Article 6 para. 3 ODPA). However, depending to the country, SCC may not be sufficient.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Personal data must be protected against unauthorized processing through adequate technical and organizational measures (Article 7 para. 1 DPA). These measures must take into account (i) the purpose of the data processing, (ii) the nature and extent of the data processing, (iii) an assessment of the possible risks to the data subjects, and (iv) the current state of the art (Article 8 para. 2 ODPA). They shall ensure the confidentiality, availability and the integrity of the data in order to ensure an appropriate level of data protection (Article 8 para. 1 ODPA).

More specifically, Article 9 para. 1 OPDA requires the following kind of measures: (i) entrance control: unauthorized persons must be denied the access to facilities in which personal data is being processed, (ii) personal data carrier control: unauthorized persons must be prevented from reading, copying, altering or removing data carriers, (iii) transport control: on the disclosure of personal data as well as during the transport of data carriers, the unauthorized reading, copying, alteration or deletion of data must be prevented, (iv) disclosure control: data recipients to whom personal data is disclosed by means of devices for data transmission must be identifiable, (v) storage control: unauthorized storage in the memory as well as the unauthorized knowledge, alteration or deletion of stored personal data must be prevented, (vi) usage control: the use by unauthorized persons of automated data processing systems by means of devices for data transmission must be prevented, (vii) access control: the access by authorized persons must be limited to the personal data that they required to fulfilment their task, and (viii) input control: in automated systems, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by which person.

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The DPA does not specifically address "security breaches" and does not provide a definition. However, data breaches are to be avoided by the technical and

organizational measures to be taken pursuant to Article 7 DPA, as these serve to prevent a breach of the confidentiality, availability or integrity of the data under the control of the controller.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

Swiss law imposes sector-specific data security obligations on, for example, financial services organizations, telecommunication providers, healthcare providers and medical researchers.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

DPA does not provide for a general obligation to notify data breaches to the regulator, affected data subjects or other third parties.

Depending on the circumstances, controllers should consider voluntarily notifying affected data subjects if a breach of personal data occurs because (i) the timely notification to affected data subjects helps them to mitigate potential harm associated with any loss or misuse of their personal data, or (ii) notifying data subjects and helping them protect themselves may decrease the risks of litigation and loss of customer trust that often occur following a data breach. Depending on the extent of the breach, it is also recommended to voluntarily inform the FDPIC in order to avoid or limit an investigation.

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

There is no overarching, stand-alone cybersecurity legislation in Switzerland. Cybersecurity is governed primarily by a patchwork of different laws and regulatory policies that explicitly or implicitly address cybersecurity.

The Ordinance on the Protection against Cyber Risks in the Federal Administration (CyRV) assigns responsibilities within the federal government and aims to strengthen the government's cyber threat capabilities. However, the CyRV does not address how to proceed in the event of a cyber-crime.

Certain regulations in the case of cybercrime are contained in the Ordinance on Internet Domains. Accordingly, operators of ".ch" and ".swiss" domains may be obliged to block the respective domain if there are reasonable grounds to suspect that it is being used to obtain sensitive data by unlawful means (phishing), to distribute malicious software (malware) or to support such actions (Article 15 of the Ordinance on Internet Domains).

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The FDPIC is the established body for monitoring compliance with the DPA. Other regulators, for example the Swiss Financial Market Supervisory Authority (FINMA) or the Federal Office of Communications (OFCOM), may play a role in enforcing data protection or cybersecurity regulations.

Further, Switzerland has established the National Cyber Security Centre (NCSC), under the leadership of the Federal Cybersecurity Delegate. The NCSC is the competence center for cybersecurity in Switzerland. It is responsible for the coordinated implementation of the national strategy for the protection of Switzerland against cyber-risks (NCS). The NCS aims to strengthen cybersecurity in Switzerland and combat cybercrime. It does not foresee the implementation of specific legislation on cybersecurity, but focuses on modernizing various laws that already exist to date.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

Under the DPA, data subjects have the following key data privacy rights:

- Right to information: Any data subject may request information on a controller's processing of his or her personal data (Article 8 para. 1 DPA). In particular, the data subject

may request information on (i) whether the controller processes personal data of the data subject, (ii) the purpose of the processing, (iii) if applicable, the legal basis for the processing, (iv) the categories of personal data processed, (v) the categories of recipients to whom the personal data is disclosed to, and (vi) the source of the personal data (Article 8 para. 2 DPA). The data subject must address the request for information to the controller in writing. The request does not have to be substantiated. As a rule, the controller must respond to the request within 30 days. In general, the controller must provide the information free of charge and in writing. The right to information may be limited or excluded only by an overriding public, or subject to certain limitations, private interest, or by a statutory provision of Swiss law. The controller must indicate the reasons why he or she has refused, restricted or deferred access to information.

- Right to rectification or deletion: Data subjects have the right to rectify or delete inaccurate personal data (Article 5 para. 2 DPA).
- Right to objection: Without justification, personal data shall not be processed against the express wish of the data subject (Article 12 para. 2 lit. b DPA). Therefore, data subjects have the right to object to the processing of their personal data.

33. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The data privacy rights are mainly enforced by way of civil litigation.

If the personal rights of the data subject are infringed by unlawful processing of personal data, the data subject may request that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed (Article 15 para. 1 DPA). Further, the data subject may claim damages, compensation for pain and suffering, and disgorgement of the profit resulting from the unlawful processing, to the extent that such profit results from the breach of the personal right of the data subject (Article 15 para. 1 DPA in conjunction with Article 28, 28a and 28l of the Swiss Civil Code). In practice, however, it is often difficult to prove damages, and Swiss courts tend to be reluctant to award damages for pain and suffering.

Further, according to Article 29 DPA, the FDPIC may investigate cases in more detail on his own initiative or at the request of a data subject or a third party if, for example, methods of processing are capable of breaching the privacy of larger number of persons (system errors). On the basis of his investigations, the FDPIC may recommend that the method of processing be changed or abandoned. If a recommendation made by the FDPIC is not complied with or is rejected by the data controller, the FDPIC may refer the matter to the Federal Administrative Court for a decision. Both the data controller and the FDPIC may appeal against the decision of the Federal Administrative Court. The data subject may appeal neither against the recommendation of the FDPIC nor against the decision of the Federal Administrative Court.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

Yes, see Question 33.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Yes, see Question 33. Data subjects must prove that they have suffered damage as a result of the unlawful processing of their personal data.

36. How are the laws governing privacy and data protection enforced?

Data subjects may enforce the regulations of Swiss data protection law in civil proceedings to the extent permitted by law (see Question 33).

In exceptional cases, private persons may be prosecuted and be fined for breaching obligations to provide information, to register data files, or to cooperate with the FDPIC (Article 34 DPA). Additionally, according to Article 35 DPA, upon complaint, a fine may be imposed on anyone who, without authorization, intentionally discloses confidential personal data or personality profiles worthy of protection that have become known to him or her in the course of his or her professional activity, insofar as this activity requires knowledge of such data (Article 35 DPA). The same penalties apply to anyone who without authorization willfully discloses confidential, sensitive personal data or personality

profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person. The unauthorized disclosure of confidential, sensitive personal data or personality profiles remains an offence after termination of such professional activities or training.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

The fines mentioned in Question 31 are up to CHF 10'000.00 (Article 34 and 35 DPA in conjunction with Article 106 para. 1 Swiss Criminal Code).

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

There are currently no guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions under the DPA.

As mentioned in Question 1, the DPA is currently being revised. However, it is not yet known whether such guidelines or rules will be published in the light of the new DPA.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

See Question 36.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

As mentioned under question 1, the DPA is currently being revised. The Ordinances However, the final ordinances have not yet been published and some ordinances are still under consultation.

Contributors

Michèle Burnier
Partner

michele.burnier@pestalozzilaw.com