# Switzerland - Data Protection Overview

**TABLE OF CONTENTS**

**August 2020**

# 1. THE LAW

## 1.1. Key Acts, Regulations, Directives, Bills

The Swiss Federal Act on Data Protection 1992 ('FDPA') is the key act regulating data protection in Switzerland. The Ordinance on the Federal Act on Data Protection ('FDPO') puts certain aspects of the FDPA into more concrete terms. For example, it sets out the specifics of notification requirements and the modalities of the right of access.

The FDPA is currently under revision (only available in German here, in French here, and in Italian here). The aim of the revision is, primarily, to align the FDPA's standard of protection with the standard of protection offered by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). The revised FDPA ('the Revised FDPA') (draft Revised FDPA only available in German here, French here and Italian here) will enter into force sometime in 2021 or at the beginning of 2022. A revised FDPO will enter into force together with the Revised FDPA.

Sector-specific data protection and security requirements set out in laws regulating businesses and organisations in certain sectors (including the healthcare, pharmaceutical, energy, telecommunications, and finance), provide more specific requirements applying to the processing of

e.g. patient personal data, bank customer data, or smart metre data. Sector-specific provisions typically supersede the provisions of the FDPA.

Swiss data protection law is rooted in the civil law protection of personality rights provided by Article 28 of the Swiss Civil Code ('the Civil Code'). In essence, the data processing principles set out in the FDPA provide for protection against infringements of personality rights (data privacy) through excessive use of personal data. Article 28 of the Civil Code remains relevant, from a privacy law perspective, where libel, slander, or defamation is the concern. Furthermore, Article 28 of the Civil Code is relevant for the protection of personality rights of legal entities.

In addition to criminal liability governed by the FDPA, a number of provisions of the Swiss Criminal Code ('the Criminal Code') are relevant in a data protection and privacy context. These include criminal law protection of a person's reputation against defamation (including libel and slander) and criminal law provisions prohibiting unauthorised recording of private conversations or wiretapping.

Note that only the German, French, and Italian versions of the Federal laws referenced above are official texts. English versions are provided only for reference purposes.

The 26 Cantons, the federal states of the Swiss Confederation, have enacted their own data protection acts. These govern the processing of personal data by Cantonal authorities.

### 1.2. Guidelines

Key non-binding guidelines issued by the Federal Data Protection and Information Commissioner ('FDPIC') include:

- Guidelines on data subjects' rights regarding the processing of personal data (only available in German here, in French here, and in Italian here);
- Guidelines on the processing of personal data by companies or organisations (only available in German here, in French here, and in Italian here);
- Guidelines on technical and organisational security measures;
- Guidelines on the processing of employees' personal data in the employment context (only available in German here, in French here, and in Italian here);
- Guidelines on the monitoring of internet and email use at the workplace (only available in German here, in French here, and in Italian here); and
- Guidelines on the processing of personal data in the healthcare sector (only available in German here, in French here, and in Italian here).

### 1.3. Case Law

The following are leading decisions of the Swiss Federal Supreme Court:

- Decision BGE 144 I 126 (Retention of telecommunications traffic data) (only available in German here);
- Decision BGE 143 I 253 (FINMA Watchlist) (only available in German here);
- Decision BGE 142 III 263 (Video surveillance system) (only available in German here);
- Decision BGE 141 III 119 (Employees' right of access) (only available in German here);
- Decision BGE 138 III 425 (Bank customers' right of access) (only available in German here);
- Decision BGE 138 II 346 (Google Street View) (only available in German here); and
- Decision BGE 136 II 508 (Logistep) (only available in German here).

---

## 2. SCOPE OF APPLICATION

### 2.1. Who do the laws/regs apply to?

The FDPA and the FDPO apply to the processing of personal data by businesses and organisations in all sectors of the economy as well as to the processing of personal data by Federal authorities. They also apply to the processing of personal data by natural persons in the context of business activities, but not in the context of personal household uses.

Chapter 3 of the FDPA only applies to the processing of personal data by businesses, organisations, and natural persons. Chapter 4 of the FDPA only applies to the processing of personal data by public authorities of the Federation (and to the processing of personal data by business or organisations performing tasks in the exercise of Federal public authority vested in them).

Sector-specific data protection and security requirements apply to businesses and organisations (e.g. regulated medical device manufacturers, hospitals, energy suppliers, banks, or telecommunications services providers). Note that the cookie-related information obligations set out in the Swiss Telecommunications Act ('TCA') apply to any business or organisation processing personal data on users' devices by means of using telecommunications services.

The Cantonal data protection acts govern the processing of personal data by public authorities of the relevant Canton (and the processing of personal data by business or organisations performing tasks in the exercise of Cantonal public authority vested in them).

### 2.2. What types of processing are covered/exempted?

The FDPA is an omnibus law governing any processing (including collection, storage, adaptation or alteration, disclosure, archiving, destruction or other use) of personal data. Processing of personal data by natural persons for personal household uses is exempted.

The FDPA does not apply to the processing of anonymous data (i.e. information that the respective holder or receiver of the information will not reasonably likely relate to an identified or identifiable individual).

---

# 3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

## 3.1. Main regulator for data protection

The FDPIC enforces the substantive provisions of the FDPA and the FDPO.

State prosecutors of the Cantons enforce criminal law provisions of the FDPA against the natural persons responsible for the violation (or against businesses or organisations, under certain circumstances). They will continue to do so under the Revised FDPA. State prosecutors also enforce the data protection law-related offences under the Criminal Code.

The data protection supervisory authorities of the Cantons enforce the Cantonal data protection acts.

In addition, private enforcement plays a role, in particular as regards injunctions banning disclosure of personal data, and the enforcement of the right of access or the right to have personal data rectified or deleted (cf. below, at section 12.3).

## 3.2. Main powers, duties and responsibilities

Under the current FDPA, the FDPIC may only issue non-binding recommendations. However, where the business, organisation, or Federal authority concerned does not agree to implement the recommendation, the FDPIC may file a complaint with the Federal Administrative Court and request that the court order the defendant to implement the recommendation.

Under the Revised FDPA, the FDPIC will have the power to issue binding decisions: The FDPIC may (*ex officio* or upon a data subject's complaint) require the respective business or organisation or Federal authority to correct, suspend, or cease certain processing of personal data, or to delete personal data entirely or partially. The FDPIC may also require the business, organisation, or Federal authority concerned to comply with specific obligations, such as to inform individuals, grant a right of access,

or to perform a Data Protection Impact Assessment ('DPIA'). In contrast to supervisory authorities in most jurisdictions where the GDPR is enforced, the FDPIC will not, however, have the power to impose administrative fines on businesses or organisations. Nor will the FDPIC have the power to impose fines on individuals.

---

## 4. KEY DEFINITIONS | BASIC CONCEPTS

**Personal Data:** The FDPA defines 'personal data' as any information relating to an identified or identifiable person. This includes information that directly identifies a (natural) person (e.g. a full name or picture showing a person's face) and information that allows identification indirectly by reference to additional information (e.g. email address, telephone number, social security number, or customer number). A 'relative' approach to identification applies. Information may qualify as personal data in the hands of one party and as anonymous data in the hands of another party. Identifiability means that the party holding or receiving the information has (or will reasonably likely gain) access to means it will reasonably likely use to identify the (natural) person directly or indirectly. To ascertain whether such identification is reasonably likely, account is taken of the costs of and the amount of time the holder or receiver of the information requires for identification, taking into consideration the technology available to such business, organisation, or natural person. Note that the current FDPA also governs the processing of information relating to an identified or identifiable legal entity. The Revised FDPA will not apply to processing of information relating to an identified or identifiable legal entity.

**Sensitive Data:** Under the FDPA, the following categories of personal data qualify as 'sensitive:'

- personal data concerning religious, ideological, political, or trade union-related views or activities;
- personal data concerning health, the intimate sphere, or the racial origin of an individual;
- personal data concerning social security measures; and
- personal data concerning administrative or criminal proceedings and sanctions.

These categories of personal data will continue to be considered sensitive under the Revised FDPA. The Revised FDPA will add two new categories:

- genetic data; and
- biometric data that uniquely identifies an individual.

**Data Controller:** The Revised FDPA will distinguish controllers and processors. Similarly, the current FDPA distinguishes owners of data filing systems and third parties processing personal data on behalf of such owner. The term 'controller' (under the Revised FDPA) refers to the business, organisation, natural person, or Federal authority that determines (alone or jointly with others) the purpose and means of the processing of personal data.

**Data Processor:** 'Processors' (under the Revised FDPA) are businesses, organisations, natural persons, or Federal authorities that process personal data on behalf (and for the purposes of) the controller.

**Disclosure:** 'Disclosure' means making personal data available; for example, by permitting access, transferral to a third party (except to processors engaged by the controllers), or publication.

**Data subject:** 'Data subject' means the individual to whom the processed personal data relates.

**Processing:** 'Processing' means any operation performed on personal data, irrespective of the means or procedures applied, and in particular the collection, storage, use, adaption or alteration, disclosure, archiving, or destruction of data.

## 5. NOTIFICATION | REGISTRATION

### 5.1. Requirements and brief description

No registration with or notification to the FDPIC is generally required. However, under the current FDPA, businesses or organisations have to register their data files with the FDPIC if they regularly process sensitive personal data or regularly disclose personal data to third parties. They are exempted from this registration obligation if they have appointed a data protection officer ('DPO') and have notified the FDPIC of such appointment. The obligation to register data files will no longer apply to business or organisations under the Revised FDPA.

## 6. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

### 6.1. Processing principles

The following processing principles are key principles and responsibilities of controllers under the FDPA. They will continue to apply under the Revised FDPA.

- **Lawfulness**: Businesses or organisations (controllers) may only process personal data that has been collected in accordance with other applicable laws. For example, processing personal data that has been collected through unlawful trespassing or wiretapping would infringe the 'lawfulness' principle. Note that, in contrast to the principle of 'lawfulness of processing' on which the GDPR is based, the processing of personal data by businesses, organisations, or natural persons is generally allowed under the FDPA. Only public authorities require a legal basis for processing. Such legal basis has to be a statutory basis laid down in Swiss law.
- **Fairness** (good faith): Controllers may only perform such processing activities as data subjects may reasonably expect. Furthermore, fairness (good faith) means that processing must be performed as described in privacy notices.
- **Transparency**: Controllers have to convey to data subjects all information necessary in order to ensure transparent data processing. The information needs to enable data subjects to exercise their rights under the FDPA. The Revised FDPA will set out in more detail the types of information that controllers need to convey to data subjects. At a minimum, they will need to inform data subjects about:
    - the identity and contact details of the controller;
    - the contact details of the DPO (if any);
    - the purposes of the processing;
    - (if any) the recipients or categories of recipients of the personal data;
    - (if the controller intends to transfer personal data internationally) the countries the controller intends to transfer personal data to and (in the absence of an adequacy decision taken by the Federal Council) based on which safeguards (e.g. Standard Contractual Clauses ('SCC') or the Swiss-US Privacy Shield); and
    - (if the controller has not obtained the personal data directly from the data subject) the categories of personal data collected and processed.
- **Purpose limitation**: Controllers may only process personal data for the specified purposes that have been notified to or are obvious to data subjects; and may only process personal data in a manner compatible with those purposes. The information about the purposes of the processing needs to be specific. Controllers also need to ensure that further processing of personal data received from other controllers is compatible with the purposes determined and communicated to the data subjects at the time of collection.
- **Proportionality**: The processing of personal data needs to be proportionate; that is, limited to what is necessary to achieve the specified purposes, considering the type of personal data concerned and the scope and duration of the processing. The data minimisation and storage limitation principles are key aspects of the proportionality principle. This means that controllers need to limit the scope of personal data collected and

processed to what is necessary for the intended purposes, and to delete personal data once it is no longer needed for the specified purposes.

- **Accuracy**: Controllers need to ensure they only process personal data that is accurate and kept up to date. They must take all reasonable steps to ensure that personal data that is inaccurate or incomplete, having regard to the purposes for which it is processed, is deleted or rectified.
- **Data security** (integrity and confidentiality): Both controllers and (under the Revised FDPA) processors are under an obligation to ensure an adequate level of data security. They are required to protect the integrity, confidentiality, and availability of personal data by means of adequate technical and organisational security measures. In assessing the appropriate level of security, controllers and processors have to account for the purpose, type, and scope of the data processing, the assessment of potential risks for data subjects, and the state-of-the-art security solutions.

If businesses and organisations process personal data in accordance with the processing principles set out above, the processing will generally be considered lawful as long as the data subject has not expressly objected to the processing. Infringements of these processing principles (e.g. processing for further purposes than those initially specified, or processing for longer than necessary for the specified purposes), or continued processing despite the data subject's objection, are breaches of personality rights of the affected data subject. In addition, disclosure of sensitive personal data to third parties without a valid ground for justification is deemed a breach of personality rights.

Breaches of personality rights are deemed unlawful unless the controller can demonstrate that the relevant processing is justified. Valid grounds for justification are:

- the data subject's consent;
- overriding public interests or private interests (including necessity for the performance of a contract or, if the controller does not disclose the personal data to third parties, to pursue legitimate business interests of the controller); or
- necessity to comply with a legal obligation laid down in Swiss law.

## 6.2 Further responsibilities of controllers

The following are further key or new responsibilities of controllers under the Revised FDPA:

- **Records of processing activities**: Under the Revised FDPA, controllers (and processors) will be required to maintain records of processing activities. Exemptions may apply in

relation to low-risk processing of personal data by businesses with less than 50 employees. The revised FDPO will lay out the specifics of this and other exemptions that may apply.

- **DPIAs**: Under the Revised FDPA, controllers will be required to perform DPIAs for intended high-risk processing of personal data. The high risk may result from the type, scope, circumstances or purposes of the processing or from the use of new technologies. A DPIA will be required under the Revised FDPA, in particular, in the case of processing on a large scale of sensitive personal data, or the systematic monitoring of publicly accessible areas on a large scale.
- **Prior consultation**: Under the Revised FDPA, a controller will be required to consult the FDPIC prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Business or organisations (private controllers) that have appointed a DPO and have involved the DPO in the DPIA may forego prior consultation of the FDPIC.

## 7. DATA PROCESSOR RIGHTS AND RESPONSIBILITIES

Controllers will continue to be primarily responsible for compliance with the Revised FDPA. Yet, in contrast to the current FDPA, the Revised FDPA will also set out legal obligations applying directly to processors (including data security obligations, restrictions on engaging sub-processors, and the requirement to maintain a record of processing activities).

## 8. DATA CONTROLLER AND PROCESSOR AGREEMENTS

The controller-to-processor relationship needs to be governed by a contract (or established by law). The controller needs to be sure that the processor only performs processing activities that the controller would also be allowed to perform and to ensure that the processor is capable of providing for adequate data security. Further, the Revised FDPA provides that a processor may only hire a sub-processor with the prior consent of the controller. The standard required by Article 28(3) of the GDPR will suffice in most circumstances for the purposes of the Revised FDPA. Thereby, parties should clarify that Switzerland is considered a member of the European Economic Area for the purposes of the data processing agreement.

## 9. DATA SUBJECT RIGHTS

Individuals have the following individual rights in relation to personal data concerning them:

- the right to receive information about the processing;
- the right of access;
- the right to rectification or deletion;
- the right to receive a copy of the personal data undergoing processing;
- the right to transfer (or have transferred) personal data to another controller;
- the right to object to the processing of the personal data; and
- the right to complain to the FDPIC.

These rights of individuals are subject to conditions and exceptions. For example, the right to receive information about the processing, or to access or receive a copy of the personal data undergoing processing may be limited, deferred, or denied to the extent necessary in order to protect the privacy interests of other data subjects or the legitimate business interests of third parties (or of the controller, if it does not disclose the personal data to third parties) that override the data subject's privacy interests. Furthermore, legal obligations of the controller such as statutory confidentiality obligation or records keeping obligations may prevent the controller from providing information or, respectively, deleting personal data.

---

## 10. DATA PROTECTION OFFICER

### 10.1. DPO – compulsory appointment (yes/no)

No. Appointing a DPO is not mandatory for businesses and organisations under the FDPA or the Revised FDPA. But the Revised FDPA incentivises the appointment of a DPO (cf. above, regarding DPIAs and prior consultations). In practice, it may also be advisable to appoint a DPO voluntarily, as compliance with documentation and notification obligations and responding to data subjects' requests under the Revised FDPA requires businesses, in practice, to establish an internal data protection function.

### 10.2. Requirements

The DPO must be independent in terms of organisation and their professional expertise. From an organisational point of view, he or she may not perform tasks that are incompatible with the tasks of the DPO (avoidance of conflicts of interest). As regards professional expertise, the controller or processor has to ensure the DPO does not receive any instructions regarding the exercise of his or her tasks.

Further, the DPO must have the professional skills and expertise necessary to perform the statutory tasks of a DPO. Basic knowledge of data protection law is generally sufficient in order to perform the tasks of advising on and monitoring compliance with data protection laws (in particular, if supported by external legal advisors), and for consultation with the FDPIC. At least as important (namely in connection with a DPIA or with regard to data security) is knowledge of the relevant technology, data flows, and business processes.

Businesses or organisations that appoint a DPO in accordance with the Revised FDPA will have to publish and provide to the FDPIC the contact details of the DPO.

---

## 11. DATA BREACH NOTIFICATION

### 11.1. General obligation (yes/no)

Yes. Under the Revised FDPA, controllers will be required to notify the FDPIC of personal data breaches that may result in a high risk for data subjects (the current FDPA does not set out any data breach notification obligations, but notification is considered a best practice). No deadline is defined for the notification. Controllers will need to notify the FDPIC as quickly as possible, i.e. without undue delay. In their notification, they will need to address the type of personal data breach, its consequences, and the measures taken or planned to remedy the breach and mitigate risks for data subjects.

Controllers are required to notify the data subjects affected by the personal data breach if such notification is necessary in order to protect the data subjects or if the FDPIC so requests.

Processors who detect a personal data breach are required to notify the controller of the breach.

### 11.2. Sectoral obligations

Data breach notification obligations that apply to regulated banks or insurance companies (in relation to customer data) or hospitals (in relation to electronic patient records) apply in addition to the obligation to notify personal data breaches under the Revised FDPA.

---

## 12. SANCTIONS

### 12.1. Administrative law enforcement

The FDPIC does not (and will not under the Revised FDPA) have the right to issue administrative fines. But the FDPIC has corrective powers. It may oblige businesses or organisations or Federal authorities to correct, suspend, or cease certain processing of personal data, or to delete personal data entirely or partially. The FDPIC may also require the business, organisation, or Federal authority concerned to comply with specific responsibilities (cf. further above, at Section 3.2.).

## 12.2 Criminal law enforcement and sanctions

The state prosecutors enforce the criminal law provisions of the FDPA. Currently, the FDPA provides that natural persons may be fined up to CHF 10,000 (approx. €9,300) if they are responsible for the violation of certain information and notification requirements under the FDPA (e.g. willfully providing false or incomplete information in response to a data subject access request).

Under the Revised FDPA, the maximum amount of the fine will be CHF 250,000 (approx. €232,420). The Revised FDPA will also extend criminal liability to the violation of additional data protection obligations under the Revised FDPA, such as failing to ensure there are sufficient guarantees for international data transfers or failure to comply with minimum data security requirements.

The Revised FDPA will also introduce criminal liability of businesses and organisations. The responsible natural persons (e.g. directors or managers) will primarily be liable. However, the business or organisation (controller or processor) may be held liable for a fine of up to CHF 50,000 (approx. €46,490) under the Revised FDPA if determining who in the organisation is responsible for the infringement would require disproportionate investigative efforts.

## 12.3 Private enforcement

The FDPA provides private rights of actions against infringements of personality rights protected under the FDPA. Of particular practical relevance is litigation concerning the exercise of the rights of access, rectification, and deletion. Yet data subjects may also claim infringement of key data privacy principles such as purpose limitation, data minimisation, and data security. The following remedies are available for claims brought under the FDPA:

- prior restraints and other injunctions preventing an imminent infringement (such as unlawful disclosure of personal data);
- removal of an existing infringement (this includes enforcement of the right to rectification or deletion);
- an order of the court requiring the controller to provide information or access;

- a declaratory judgment (if the infringement continues to affect the privacy interests of the data subject); and
- claims for compensatory damages, moral damages, and disgorgement of profits.

---

# 13. ADDITIONAL RELEVANT TOPICS

## 13.1. Data Transfers and Outsourcing

Under the current FDPA, the FDPIC publishes a list of states that, according to the FDPIC's assessment, provide an adequate level of data protection. Under the Revised FDPA, the Federal Council will adopt adequacy decisions in relation to jurisdictions that provide an adequate level of protection. The Federal Council will (just as the FDPIC has done in the past) likely follow the European Commission's lead and consider adequate those jurisdictions in relation to which the European Commission has adopted an adequacy decision.

Appropriate safeguards are required in order to transfer personal data to states without an adequate level of protection. Appropriate safeguards include, under the Revised FDPA: SCC issued, approved or recognised by the FDPIC, Binding Corporate Rules approved by the FDPIC or a competent data protection supervisory authority in a state that provides adequate protection, or (subject to prior notification to the FDPIC) contractual clauses incorporated into a controller-to-processor data processing agreement. In addition, the Revised FDPA provides for derogations for data transfers in specific situations, such as where the transfer is directly related to the conclusion or the performance of a contract between the data subject and the controller.

The above rules on data transfers also apply in an outsourcing context, where a controller in Switzerland engages a processor in another state, or where a processor in Switzerland engages a sub-processor in another state. In addition, controller-to-processor relationships and processor-to-sub-processor relationships have to be governed by a data processing agreement.

If controllers rely on (controller-to-processor) SCC for the transfer of personal data to processors in a state in relation to which the Federal Council has not adopted an adequacy decision, they may, in principle, forego entering into a separate data processing agreement. Yet in most circumstances, it will be more practical to enter into a data processing agreement and incorporate the SCC therein. SCC must not be changed and thus offer no flexibility for tailor-made clarifications of the roles of each party as well as the implementation of sufficient controls over the processing activities carried

out by the processor (such as instruction, inspection, and audit rights, limitations on engaging sub-processors, as well as duties to cooperate and to implement adequate organisational and technical security measures).

### 13.2. Employment

Generally, employers may only process employee personal data to the extent the processing relates to the workplace. This includes processing that is necessary for the performance of the employer's obligations to the employee under the employment contract, for compliance with statutory obligations, or for the purposes of legitimate interests of the employer or third parties that have a sufficient connection to the workplace (e.g. the enforcement of legal claims, measures ensuring safety at work or information security, fleet management, or marketing of professional services performed by the employee). Obtaining the employees' consent is typically not necessary (and will not be valid unless the employee has a real choice).

Employees have a duty of loyalty to their employers. This means that employees have to tolerate certain restraints on their privacy interests. At the same time, employers have a duty of care to their employees. Even if employees are under a loyalty obligation, employers have to process employee personal data in ways that are least intrusive to the privacy interests of their employees (principle of proportionality). Thereby, of particular importance is adequate information of the employees about the functioning and purposes of, for example, fleet management, internet use monitoring, or video surveillance systems that the employer intends to use, and about the employees' rights in connection with the processing of personal data for such purposes.

### 13.3. Data Retention

Controllers have to delete or sufficiently de-identify (i.e. render anonymous) personal data once they no longer need it for the specified purposes, or in order to pursue legitimate interests (such as enforcement of legal claims) or to comply with legal obligations (such as records-keeping obligations).

---

## 14. OTHER SPECIFIC JURISDICTIONAL ISSUES

### 14.1. Territorial reach

The principle of effects determines the FDPA's territorial scope. In other words, the FDPA applies to the processing of personal data that has actual or potential effects in Switzerland. This includes processing activities that are conducted or initiated outside of Switzerland but actually or potentially adversely affect the privacy rights of individuals in Switzerland. According to established case law, this territorial scope already applies to investigation proceedings of the FDPIC under the current FDPA. The Revised FDPA will codify this case law. Further, the Revised FDPA may apply, in accordance with the principle of effects under private international law, in private enforcement.

### 14.2. Representative

Under the Revised FDPA, business or organisations (private controllers) established outside of Switzerland will have to appoint a representative in Switzerland under certain conditions. In accordance with the current draft, they will be required to do so if they regularly perform high-risk and large-scale processing of personal data in connection with the offering of goods or services in Switzerland, or in connection with the monitoring of individuals' behaviour taking place in Switzerland.

### 14.3. New developments

Data-driven business models have become prevalent in recent years. Consumers acknowledge the value of these business models but are increasingly concerned about their privacy in a digital economy. In particular, decision-making based on algorithms and big data analysis create a perception of losing control over one's personal data. Further, in the wake of various high-profile data breaches, information security has become an important topic.

On the legislative landscape, the completion of the revision of the FDPA will likely further increase awareness in the next few years. Also, it is expected that data protection and security provisions in sector-specific laws and regulations concerning the use of data in highly regulated sectors will continue to receive more attention.

The Revised FDPA will empower the FDPIC to require controllers and processors to change their data processing operations. Yet the effectiveness of the FDPIC's greater enforcement powers will largely depend on the resources made available to the FDPIC. These have so far been rather limited. Even with extended resources, it remains to be seen whether enforcement of the Revised FDPA by the FDPIC proves effective, particularly given that the FDPIC may not issue administrative fines. State prosecutors tend to have other enforcement priorities and a lack of sufficient data protection know-

how. Enforcement of the criminal law provisions of the Revised FDPA, therefore, may also remain limited. Private enforcement remains costly due to limited pre-trial disclosure, and because opportunities for collective legal action are very limited.