ICLG

The International Comparative Legal Guide to:

# Data Protection 2018

## 5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

**Contributing Editors**
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

**Sales Director**
Florjan Osmani

**Account Director**
Oliver Smith

**Sales Support Manager**
Toni Hayward

**Sub Editor**
Oliver Chang

**Senior Editors**
Suzie Levy
Caroline Collingwood

**Chief Executive Officer**
Dror Levy

**Group Consulting Editor**
Alan Falach

**Publisher**
Rory Smith

**Published by**
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

**GLG Cover Design**
F&F Studio Design

**GLG Cover Image Source**
iStockphoto

**Printed by**
Ashford Colour Press Ltd
June 2018



**ISBN** 978-1-912509-15-7
**ISSN** 2054-3786

**Strategic Partners**

MIX
Paper from responsible sources
FSC® C011748

## General Chapters:



## Country Question and Answer Chapters:



**Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720**

# Switzerland

Lorenza Ferrari Hofer

Pestalozzi

Michèle Burnier

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

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").

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.

### 1.2 Is there any other general legislation that impacts data protection?

Every Swiss canton has its own data protection statutes with respect to data processing of cantonal public authorities.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The Swiss banking secrecy and guidelines thereto impact data protection when bank customer data are processed. Furthermore, secrecy obligations, such as patient secrecy regarding health data as set out in article 321 of the Swiss Criminal Code, have an impact on when respective data are processed. Particular rules concerning data retention and processing also apply in the telecommunication sector.

### 1.4 What authority(ies) are responsible for data protection?

The Federal Data Protection and Information Commissioner ("FDPIC") is the relevant authority if personal data are processed by federal authorities, individuals and legal entities. The respective Cantonal Data Protection and Information Officer in each canton is the responsible authority if personal data are processed by public authorities of the respective canton.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  All information relating to an identified or identifiable natural or legal person (see article 3 lit. a and b DPA).

- **"Processing"**

  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 (see article 3 lit. e DPA).

- **"Controller"**

  There is no statutory definition, as the term is not explicitly used in the DPA. The FDPIC defines "Data Controller" or "Data Exporter" in its template outsourcing agreement as follows: the natural or legal person, public authority, agency or any other body established in Switzerland which alone or jointly with others determines the purposes and means of the processing of personal data and which transfers such data (to another country) for the purposes of its processing on his/her behalf.

- **"Processor"**

  There is no statutory definition, as the term is not explicitly used in the DPA. The FDPIC defines "Data Processor" or "Data Importer" in its template outsourcing agreement as follows: natural or legal person, public authority, agency or any other body (established in another country) which agrees to receive personal data from the Data Exporter for the purposes of processing such data on behalf of the latter after the transfer in accordance with his/her instructions.

- **"Data Subject"**

  Natural or legal persons whose data are processed (see article 3 lit. b DPA). It is important to emphasise that the DPA does not only protect personal data of natural persons as most other data protection laws, but also personal data of legal persons.

- **"Sensitive Personal Data"**

  Data on: 1) religious, ideological, political or trade union-related views or activities; 2) health, the intimate sphere or racial origin; 3) social security measures; and 4) administrative or criminal proceedings and sanctions (see article 3 lit. c DPA).

- **"Data Breach"**

  There is no statutory definition, as the term is not explicitly used in the DPA.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Data Owner"**

    The term used in the DPA is "Controller of the Data File", which is any private person or federal body that decides on the purpose and content of a data file (see article 3 lit. i DPA).
  - **"Pseudonymous Data"**

    There is no statutory definition. Pseudonymous data are 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. Anonymous data are data for which the relation to a natural or legal person is entirely removed.
  - **"Personality Profile"**

    A collection of data that permits an assessment of essential characteristics of the personality of a natural person (see article 3 lit. d DPA).
  - **"Data Files"**

    Any set of personal data that is structured in such a way that the data are accessible by the data subject (see article 3 lit. g DPA).

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The DPA applies as soon as data are processed in Switzerland. Thus, if personal data are archived in Switzerland (e.g., in a cloud), the DPA will apply – even though no data were collected in Switzerland and the data subjects are not located in Switzerland.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The collection of personal data and in particular the purpose of its processing must be evident to the data subject (see article 4 para. 4 DPA).
- **Lawful basis for processing**

  Personal data may only be processed lawfully (see article 4 para. 1 DPA).
- **Purpose limitation**

  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 (see article 4 para. 3 DPA).
- **Data minimisation**

  There is no such principle set out in the DPA, but the FDPIC considers that it is part of the general principle of proportionality.
- **Proportionality**

  Data processing must be carried out in good faith and must be proportionate (see article 4 para. 2 DPA).
- **Retention**

  This is not a key principle set out in the DPA. However, the principle of proportionality requires that personal data are only retained as long as it is necessary with respect to the purpose of the data processing. General data retention requirements are not set forth in the DPA, but rather in the Swiss Code of Obligations or sector-specific regulations.
- *Other key principles – please specify*

  There are no other key principles.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have 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/her is being processed (see article 8 para. 1 DPA; exceptions are mentioned in article 9 DPA).
- **Right to rectification of errors**

  Any data subject may request that incorrect data be corrected (see article 5 para. 2 DPA).
- **Right to deletion/right to be forgotten**

  Any data subject may request that incorrect data be deleted (see article 5 para. 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 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 para. 1 DPA). It is important to note that data processing may be blocked by preliminary injunctions.
- **Right to restrict processing**

  There is no such principle set out in the DPA.
- **Right to data portability**

  There is no such principle set out in the DPA.
- **Right to withdraw consent**

  According to article 12 para. 2 lit. 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 (i.e., marketing newsletters) in article 3 lit. 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 own initiative or at the request of a third party (see article 29 para. 1 DPA).
- *Other key rights – please specify*

  There are no other key rights.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Cross-Border Data Transfer: if personal data are transferred to a country that has no adequate data protection laws in force, additional safeguards are necessary. Safeguards are, for example, data transfer agreements or group-wide data protection policies (for transfers within a group of companies). The FDPIC must be informed about these safeguards prior to transborder disclosure (see article 6 para. 3 DPA and article 6 para. 1 ODPA).

Registration of Data Files with the FDPIC: federal bodies must register their data files with the FDPIC (see article 11a para. 2 DPA). Private persons must register their data files with the FDPIC only if: 1) they regularly process sensitive personal data or personality profiles; or 2) they regularly disclose personal data to third parties (see article 11a para. 3 DPA). Exceptions from the registration duty are set out in article 11a para. 5 DPA and in article 4 ODPA (for example, if the respective legal entity has appointed an internal Data Protection Officer who monitors compliance with data protection laws).

### 6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registration/notification must include both specific but also general information (for further details, see the answer to question 6.5 below).

### 6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

See the answer to question 6.1 above. The registration of data files is made per data file.

### 6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Generally, the local legal entity is the Data Controller who transfers personal data pursuant to the DPA abroad (see the definition in the answer to question 2.1 above) and/or is the Controller of the Data File (see the definition in the answer to question 2.1 above).

Foreign entities domiciled outside of Switzerland may be qualified as Controllers of the Data File in the sense of the DPA. However, the FDPIC is not able and does not enforce the DPA in the case of a foreign legal entity domiciled outside of Switzerland because of the principle of territoriality. In case a foreign legal entity is the Controller of the Data File with personal data of Swiss data subjects, the FDPIC may investigate whether a legal entity in Switzerland is co-controller of the respective data file. The representative or branch office of a foreign Controller of the Data File is not automatically subject to the registration obligation. The representative or branch office of a foreign entity is usually not to be qualified as Controller of the Data File, since often they do not have the power to decide on the content or purpose of a data file.

### 6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Cross-Border Transfers: no detailed information is required if the standard contractual clauses of the EU or the FDPIC are used, but the communication must include the country to which the data will be transferred and the name(s) of the data recipients(s). Otherwise, the copy of the respective contract clauses must be disclosed to the FDPIC.

Data Files: information regarding the notifying entity, contact person for information requests, categories of personal data, categories of data subjects, categories of data recipients, categories of persons having access to the data files and processing purposes must be disclosed. The FDPIC provides a template registration form on its website.

### 6.6 What are the sanctions for failure to register/notify where required?

Upon complaint, the respective entities or individuals may be fined if they wilfully infringed the registration obligation (see article 34 para. 2 DPA). The fine can be up to CHF 10,000.

### 6.7 What is the fee per registration/notification (if applicable)?

There is no fee for the registration of data files or cross-border transfer notifications.

### 6.8 How frequently must registrations/notifications be renewed (if applicable)?

The registration must be renewed as soon as the notified information changes. There is, however, no strict deadline and the update can be executed electronically.

### 6.9 Is any prior approval required from the data protection regulator?

There is no such obligation. Regarding federal and cantonal authorities, such approval obligations may arise out of specific public law.

### 6.10 Can the registration/notification be completed online?

Yes, the notification can be completed online, but the confirmation must be signed by an authorised representative and returned by courier to the FDPIC.

### 6.11 Is there a publicly available list of completed registrations/notifications?

Yes, the publicly available list can be accessed via the website of the FDPIC (https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/entreprises/anmeldung-einer-datensammlung.html).

**6.12 How long does a typical registration/notification process take?**

The registration process usually takes between one to two weeks.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

The appointment of a Data Protection Officer is optional.

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

There are no sanctions.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?**

There are no specific provisions in the DPA in this regard; thus, the general rules and principles based on the Swiss Code of Obligations will apply.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes, a single officer may cover multiple entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Independence (performs his/her function without instructions from the Controller of the Data File); sufficient resources with respect to skills and time; sufficient personal and organisational power (as he/she must have access to all data files, data processing and information thereto) (see article 12a para. 2 and article 12b para. 2 ODPA).

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

Monitoring the processing of personal data and suggesting corrective measures if data protection regulations should not be complied with, and maintaining a list of all data files (see article 12b para. 1 ODPA).

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

Yes (see article 12a para. 1 lit. b ODPA).

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

No, there is no such requirement under the DPA.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes, an agreement with the processor is required.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

The agreement must not necessarily be in writing, but it must ensure that the data are processed only in the manner permitted for the instructing party itself and is not prohibited by a statutory or contractual duty of confidentiality. In particular, the instructing party must ensure that the processor guarantees data security.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (E.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)**

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

Regarding mass emails and text messages, article 3 lit. o of the Unfair Competition Act requires that such communication is only sent with the prior consent of the recipients and with 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 it has purchased before 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.

**9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.)**

Article 3 lit. u of the Unfair Competition Act prohibits marketing communication via telephone, email and fax if the recipient has declared in any telephone registry that he/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.

**9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, they also apply to marketing sent from other jurisdictions.

**9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

In Switzerland, it is the State Secretariat for Economic Affairs ("SECO") which is the competent authority to file a claim in case of violation of the interests of many persons (article 10 para. 3 of the Unfair Competition Act). In addition, the FDPIC regularly issues guidelines on data protection aspects of marketing practices.

**9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

Yes, it is lawful to purchase marketing lists from third parties. The "SDV Schweizer Dialogmarketing Verband" is the leading association regarding dialogue marketing in Switzerland. The association's members are bound by an ethics code, which is accessible by the public (http://sdv-konsumenteninfo.ch/selbstregulierung/2012_sdv_ehrenkodex/).

**9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

In case of intentional misconduct, the respective entity (respectively, the responsible person) may be sanctioned, upon request, with a prison term of up to three years or a monetary penalty of up to CHF 1,080,000 (see article 23 of the Unfair Competition Act). The effective sanctions would, of course, be much lower than the maximum penalties. There is no penalty in case of a negligent misconduct.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Swiss law does not require an explicit opt-in regarding cookies. It is sufficient to inform the website users about cookies, the data processed by cookies, the purpose of processing and opt-out mechanisms (see article 45c of the Swiss Telecommunication Act).

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No, there is no distinction between different types of cookies.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No. The FDPIC investigates new trends regarding cookies on a regular basis but has not taken any action, since cookies are not regulated in the DPA.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

A fine not exceeding CHF 5,000 for non-compliant cookies policy on websites of Swiss providers (see article 53 of the Telecommunication Act).

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

International or cross-border disclosure means any transfer of personal data abroad, including allowing examination (e.g., of an online database), transfer or publication (see article 3 lit. f DPA). Personal data must not be disclosed abroad if the personal integrity of the persons concerned would thereby be seriously harmed (see article 6 para. 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 are disclosed.

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.

**11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The assumption that personal integrity is 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 para. 2 lit. a to lit. 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 General Data Protection Regulation 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 para. 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 para. 2 lit. 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 as well as 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 para. 2 lit. a to f DPA is satisfied:

- sufficient safeguards, in particular contractual clauses, 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 are 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 para 2 lit. a DPA. The use of the EU standard contractual clauses also facilitates the notification of the cross-border transfer to the FDPIC (see the answer to question 11.3 below).

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

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 para. 2 lit. a DPA) have been concluded or that data protection rules within the group of companies (article 6 para. 2 lit. 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 para. 3 DPA and article 6 para. 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.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

There are no specific legislation or provisions under Swiss law on whistle-blowing as such. Any whistle-blower hotlines must, however, comply with the general requirements of the DPA. 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 civil (e.g., termination of his/her job, potential damages) and criminal (e.g., offences due to false allegations, industrial espionage) sanctions. There are no restrictions as such as to what can be reported to the 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 profile must be registered with the FDPIC, even if the persons concerned are aware of the processing. 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 are data collections by companies which have appointed an internal Data Protection Officer (see the answer to question 6.1 above). Swiss doctrine is mainly of the opinion that companies with whistle-blower hotlines do not have to register the respective data collections, because there are usually no sensitive personal data or personality profiles of employees among such data and, even if there is 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. 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/her whistle-blowing activities may have before using the hotline.

**12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?**

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 para. 4 DPA (see the answer to question 4.1 above). 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.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

No, there is no general requirement to register/notify or obtain prior approval for the use of CCTV. However, if a CCTV also records activities on public ground (e.g., it records activities on a private parking lot but also covers the nearby public walkway), cantonal or local data protection laws may require separate approval from the cantonal authorities.

As the use of CCTV must be transparent for the persons concerned, they must be informed about the use of CCTV prior to accessing the surveilled premises, e.g., by a visible sign.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Yes, the use of CCTV must respect the general principles of the DPA; in particular, the principle of proportionality. Therefore, it is necessary

to weigh up the relevant interests in each case. Further, CCTV by private persons must be strictly limited to their own premises.

## 14 Employee Monitoring

### 14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

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

Anonymous monitoring (including monitoring of search strings) of, e.g., employees' use of company-provided information technology according to email and internet user guides or other policies is permissible. Pseudonymous monitoring (i.e., an abbreviation for 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 via monitoring policies.

Systematic and permanent monitoring of the information technology use of specific employees is not permitted, unless: (a) the employee has consented thereto; or (b) if there is no consent, then the following requirements have to be fulfilled: (i) justified suspicion of a criminal offence; (ii) monitoring and reading of emails is necessary to confirm or dispel suspicion; (iii) conserving evidence; and (iv) 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 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 (e.g., 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 pre-defined 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.

### 14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

See the answer to question 14.1 above: yes, prior transparent information is required; however, consent is generally not necessary.

### 14.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

The representatives of the employees in a company have a right to timely and comprehensive information by the company 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.

## 15 Data Security and Data Breach

### 15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, according to article 7 para. 1 DPA, "personal data must be protected against unauthorised processing through adequate technical and organisational measures".

Moreover, article 8 ODPA provides details on the level of security: anyone who, as a private individual, processes personal data or provides a data communication network shall ensure the confidentiality, availability and integrity of the data in order to ensure an appropriate level of data protection.

(1) In particular, he/she shall protect the systems against the following risks:
   a) unauthorised or accidental destruction;
   b) accidental loss;
   c) technical faults;
   d) forgery, theft or unlawful use; and
   e) unauthorised alteration, copying, access or other unauthorised processing.

(2) The technical and organisational measures must be adequate. In particular, they must take account of the following criteria:
   a) the purpose of the data processing;
   b) the nature and extent of the data processing;
   c) an assessment of the possible risks to the data subjects; and
   d) the technological state of the art.

(3) These measures must be reviewed periodically.

Finally, article 9 ODPA states:

(1) The Controller of the Data File shall, in particular for automated processing of personal data, take the technical and organisational measures that are suitable for achieving the following goals, in particular:
   a) entrance control: unauthorised persons must be denied access to facilities in which personal data are being processed;
   b) personal data carrier control: unauthorised persons must be prevented from reading, copying, altering or removing data carriers;
   c) transport control: on the disclosure of personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented;
   d) disclosure control: data recipients to whom personal data are disclosed by means of devices for data transmission must be identifiable;
   e) storage control: unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data must be prevented;
   f) usage control: the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented;
   g) access control: the access by authorised persons must be limited to the personal data that they require to fulfil their task; and
   h) 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.

(2) The data files must be structured in a way that data subjects are able to assert their right of access and their right to have data corrected.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

No, there is no statutory duty to do so. However, based on the general principles of the DPA, e.g., the transparency principle, it is advisable to notify the data subjects about such a breach.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

See the answer to question 15.2 above.

**15.4 What are the maximum penalties for data security breaches?**

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.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

| Investigatory Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Monetary penalty notices | This is not applicable. | This is not applicable. |
| Recommendations | The FDPIC can investigate cases and request the production of files, obtain information and arrange for processed data to be shown to him.<br>If the investigation reveals that the DPA is being breached by federal bodies, the FDPIC can recommend that the federal body concerned change the method of processing or abandon the processing. The FDPIC informs the department concerned or the Federal Chancellery of his recommendation. If a recommendation is not complied with or is rejected, 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.<br>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 of the receipt of the recommendation, the legal person must inform the FDPIC on whether it accepts and implements the recommendation or whether it rejects it. In case of a rejection, the FDPIC may bring the case to the Swiss Federal Administrative Court. | This is not applicable. |
| Enforcement notices | This is not applicable. | This is not applicable. |
| Prosecution | This is not applicable. | This is not applicable. |

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The FDPIC can issue recommendations regarding the set-up of specific processing activities. These may include the recommendation to ban 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 a federal court. The court's decision will be binding for the parties, subject to appeal to the Federal Supreme Court.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

The FDPIC issues its recommendations on a regular basis and publishes them on his website (see the answer to question 18.1 below regarding current cases).

**16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?**

Yes, the FDPIC also uses its power against companies established in other jurisdictions provided that a predominant connection to Switzerland exists. Based on this principle, the FDPIC, e.g., performed an investigation and issued recommendations in the context of Google Street View against Google, Inc. (together with Google's Swiss subsidiary) as well as in the context of Windows 10 against Microsoft Corporation (www.edoeb.ch).

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

It depends on whether these 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 para. 2 lit. c DPA).

If a Swiss company is directly approached by a foreign law enforcement agency, the request must be qualified as outside of a pending proceeding and the DPA must be complied with. The legal person may only disclose the information and personal data to the foreign authority if the DPA is complied with, in particular with article 6 DPA regarding cross-border data transfers.

The so-called Swiss blocking statutes (e.g., articles 271 and 273 of the Swiss Criminal Code) are most relevant in this context. Due to the blocking statutes, companies within Switzerland 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 members of the board might be sanctioned with a fine or imprisonment.

**17.2 What guidance has/have the data protection authority(ies) issued?**

The FDPIC has issued a guidance regarding this subject matter. Basically, the guidance comes to the same conclusions as set out in the answer to question 17.1 above.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

The Swiss Federal Supreme Court dealt with the applicability of data protection issues in international mutual legal assistance in administrative and tax matters. The Swiss Federal Supreme Court ruled that Swiss authorities must take into account the protection of third parties not directly concerned by requests of international mutual legal assistance (such as (former) employees, attorneys, notaries, managers, etc.). Therefore, it is necessary to redact the names of third parties not concerned by the request of international mutual legal assistance. Only if it is necessary to divulge the name in order to comply with the request, a name may be communicated. In tax matters the name may only be disclosed if the name is necessary to clarify the fiscal situation of the taxpayer. Thus, the principle is that the name of third parties not concerned by a request of international mutual legal assistance must not be communicated (Decision 2C_640/2016 of 18 December 2017). Furthermore, if the name of third parties must be communicated, such third party must be informed about such communication and awarded the status of a party to the proceedings (Decision 2C_792/2016 of 23 August 2017).

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

The following hot topics are currently a focus:

- Swiss-US Privacy Shield.
- Revision of the DPA.
- Revision of the legal basis for the surveillance by insurers.
- Big Data, in particular for healthcare research and platforms.
- CCTV monitoring.
- Data protection and personalised healthcare.
- Data protection and drones used by individuals for private purposes.
- Dashcams (small video recorders often used in cars).
- Transmission of data to US authorities based on the US Program for Swiss banks (ongoing decisions from the Swiss Federal Supreme Court).

After the European Commission adopted the EU-US Privacy Shield, Switzerland entered into negotiations in order to enter into a similar agreement. In 2017, Switzerland adopted the Swiss-US Privacy Shield (https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows/transfer-of-data-to-the-usa.html).

In September 2017, the Federal Council submitted a draft of the revised DPA to parliamentary discussions, which are currently

ongoing. It is not yet clear when the revised act will come into effect. The goal of this revision is, among others, to strengthen data protection provisions to reflect evolving technological and social circumstances. In this respect, a key objective is to align Swiss data protection laws with European legislation (Regulation (EU) 2016/679 and Directive 2016/680) in order to facilitate continued transborder data flows and to comply with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention ETS No. 108). Further, companies will be obliged to take steps to prevent potential data breaches whenever personal data are processed.



**Lorenza Ferrari Hofer**
Pestalozzi
Loewenstrasse 1
8001 Zurich
Switzerland

*Tel:* *+41 44 217 92 57*
*Email:* *lorenza.ferrari@pestalozzilaw.com*
*URL:* *www.pestalozzilaw.com*

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 cooperation 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 front of Swiss courts, arbitral tribunals and regulatory authorities. In addition, Lorenza Ferrari Hofer 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.

Lorenza Ferrari Hofer regularly lectures and publishes in the fields of international licensing and technology transfer, and in several areas of unfair competition, data protection law and intellectual property law. She is consistently recommended by the leading directories of the legal profession, such as *The Legal 500*, *Chambers & Partners*, *Who's Who Legal*, *WIPR Leaders* and *IAM*.

Her professional languages are German, Italian, English and French.

**Michèle Burnier**
Pestalozzi
Cours de Rive 13
1204 Geneva
Switzerland

*Tel:* *+41 22 999 96 00*
*Email:* *michele.burnier@pestalozzilaw.com*
*URL:* *www.pestalozzilaw.com*

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 telecommunication as well as administrative and contract law. She regularly represents clients before Swiss civil, administrative and/or criminal courts.

She has years of experience in negotiating and drafting complex IP agreements. Michèle Burnier is a member of various national and international organisations, such as AIPPI, INTA, ASA, LIDC and LES (member of the board of the Swiss national group), and she is Chairman of the first Chamber of the Swiss Commission for Fair Advertising (CSL). In addition, Michèle Burnier frequently lectures in seminars in the fields of intellectual property law and unfair competition, also in cooperation with the Swiss Intellectual Property Institute.

Her professional languages are French, German, English and Italian.

PESTALOZZI
ATTORNEYS AT LAW

Pestalozzi supports international and domestic clients in all aspects of Swiss law from our offices in Zurich and Geneva. The firm is known for integrity, the highest quality standards and proven effectiveness.

Clients benefits from the know-how of over 120 partners, attorneys and support staff. With practice groups and expertise in all areas of business law, Pestalozzi forms customised teams to meet every challenge. Pestalozzi's contacts include an international network of lawyers who give you access to top-quality law firms in jurisdictions worldwide.

The care of clients is the focus of everything we do at Pestalozzi, supported by the diversity of our people and a dynamic company culture that ensures a creative, practical and effective response in every case.

Pestalozzi's main clients are large domestic and foreign corporations. We also assist medium-sized companies and private individuals. The broad range of sectors it serves includes financial services as well as a vast array of industries ranging from automobiles to watches.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com