ICLG

The International Comparative Legal Guide to:

Data Protection 2017

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

Contributing Editors
Anita Bapat and Aaron P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating 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
May 2017

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Chapter 32

Switzerland

Michèle Burnier

Lorenza Ferrari Hofer

Pestalozzi Attorneys at Law Ltd.

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 (Data Protection Act, hereinafter 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 Data Protection Directive, the EU 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.

1.4 What is the relevant data protection regulatory authority(ies)?

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 relevant 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 articles 3 lit. a and b DPA).
- "**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).
- "**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).
- "**Data 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 behalf.
- "**Data 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 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.

- *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 Key Principles

3.1 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.
- **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*

  None.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Any person may request information from the controller of a data file as to whether data concerning them is being processed (see article 8 para. 1 DPA; exceptions are mentioned in article 9 DPA).
- **Correction and deletion**

  Any data subject may request that incorrect data be corrected or deleted (see article 5 para. 2 DPA).
- **Objection 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.
- **Objection 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.
- **Complaint to relevant data protection authority(ies)**

  The Commissioner 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 none.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific 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 art. 6 para. 1 ODPA). If the standard contractual clauses of the EU or the FDPIC are used, it is sufficient to inform the FDPIC about this use in a general way.

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 person has appointed an internal data protection officer who monitors compliance with data protection laws).

5.2 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 5.1 above. The registration of data files is made per data file.

5.3 Who must register with/notify the relevant data protection authority(ies)? (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 files (see the definition in the answer to question 2.1 above).

Foreign entities domiciled outside of Switzerland may be qualified as controllers of data files 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 a 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.

5.4 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 in 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. The registration may also be executed electronically.

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

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

5.6 What is the fee per registration (if applicable)?

There is no fee for the registration of data files.

5.7 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.

5.8 For what types of processing activities is 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.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

See the answer to question 5.8 above.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer is optional.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

There are no sanctions.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Data files must not be registered with the FDPIC anymore (see article 11a para. 5 DPA).

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

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

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

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

6.6 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 of the ODPA).

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

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 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 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.

7.2 Is 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.

7.3 Are companies required to screen against any "do not contact" list or registry?

Yes. Article 3 lit. u of the Unfair Competition Act prohibits marketing communication via telephone, email and fax if the recipient has declared in the telephone registry that he does not wish to receive such communication. In addition, there are several private "do not contact" lists which many companies respect but which are not mandatory.

7.4 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.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

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).

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

Neither implied nor explicit consent is necessary for cookies.

7.7 To date, has 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 did not take any action, since cookies are not regulated in the DPA.

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

A fine not exceeding CHF 5,000, (see article 53 of the Telecommunication Act).

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

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.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

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 have implemented the EU directive on data protection 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 8.3 below).

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they 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 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.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

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 (see the answer to question 16.2 below). Currently, the protection of the employee (whistle-blower) is very weak. The employee is 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 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 her/his whistle-blowing activities may have before using the hotline.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, 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 3.1 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.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

See the answer to question 9.1 above: there is no requirement for registration/notification of whistle-blower hotlines unless certain types of personal data are processed or data are regularly disclosed to third parties.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Yes. 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 her/his whistle-blowing activities may have before using the hotline.

9.5 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 a whistle-blower hotline may have an impact on employee performance, employee representatives need to be kept up to date on the whistle-blower hotline. However, there is no requirement to consult any entities.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?

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 by the cantonal authorities.

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

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 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 which 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.

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

See the answer to question 10.2 above: yes, prior transparent information is required, however, consent is generally not necessary.

10.4 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 CCTV and employee monitoring may have an impact on employee performance, employee representatives need to be kept up to date on these subjects. However, there is no requirement to consult any entities.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, there is no such duty.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, it is permitted. There are no specific statutory provisions, however. Generally, the provisions of the DPA have to be complied with, e.g., the data subjects must be transparently informed about the fact that the data are processed in the cloud and the necessary security and organisational measures must be implemented. Furthermore, the transfer and processing of personal data in the cloud is qualified as data processing outsourcing in the sense of article 10a DPA which requires a written data processing agreement between the data controller and the data processor (cloud provider).

The written agreement must include provisions on instruction and monitoring of the processor and audit rights on behalf of the data controller. The FDPIC recommends the use of either the EU standard contractual clauses for transfer of personal data from data controller to data processor, or the template agreement for outsourcing of data processing of the FDPIC.

Finally, the right to obtain information and the right to have data deleted or corrected must be respected both by the data controller and the data processor.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no requirements which relate specifically to providers of cloud-based services. The provisions of the DPA, in particular the provisions relating to data security, are applicable and consequently, the controller must ensure that the processor has implemented adequate technical and organisational measures against unauthorised processing of personal data. Moreover, the controller must ensure that the processor can only process personal data in the way the controller is able to. Sector-specific additional rules may be applicable such as in the banking or healthcare sector.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, the utilisation of big data and analytics is permitted and the general provisions of the DPA apply. There is no specific law or binding guidance relating to big data and analytics.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Article 7 para. 1 DPA states that "personal data must be protected against unauthorised processing through adequate technical and organisational measures".

Moreover, article 8 of the 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 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 of the 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 required 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.

13.2 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.

13.3 Is there a legal requirement to report data breaches to individuals? 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 13.2 above.

13.4 What are the maximum penalties for 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.

14 Enforcement and Sanctions

14.1 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. 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. 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 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.

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

The FDPIC issues his recommendations on a regular basis and publishes them on his website (see the answer to question 16.1 below regarding current cases).

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction 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 cannot (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.

However, the so-called Swiss blocking statutes (e.g. articles 271 and 273 of the Swiss Criminal Code) are more important than the DPA in this context. Due to the blocking statutes, companies within Switzerland cannot just simply comply with foreign e-discovery requests (even if the data transfer abroad were in compliance with the DPA). 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.

15.2 What guidance has 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 15.1.

16 Trends and Developments

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

There are several decisions of the Swiss Federal Administrative Court dealing with the access right to personal data collected and processed by federal authorities.

More relevant with regard to data processing by natural and legal persons are the following cases dealing with (i) the disclosure of personal data to U.S. authorities in connection with the tax dispute between Swiss banks and the United States, (ii) the CCTV monitoring by a private company, and (iii) the surveillance of an insured by the insurer which hired private investigators to conduct secret surveillance.

In June 2014, a Swiss bank participating to the Program for non-prosecution agreements and non-target letters for Swiss banks ("US Program") informed a law firm company and two lawyers working for this company of its intention to transmit to the U.S. Authorities their names in relation with seven bank accounts linked with U.S. clients. The law firm and the two lawyers opposed to the transmission. The Supreme Court held that the bank could not rely on justifications according to article 6 para. 2 DPA. In its decision, the Court stressed that the overriding interest (i) must be examined based on a case-by-case principle, and (ii) must (still) exist at the date of the judgment. In the case at hand, the Supreme Court considered that the bank did not establish that the non-delivery of the names of claimants would lead to an escalation of the tax dispute between Swiss banks and the United States. The Court held therefore that there are no overriding public interests which would allow the data transfer.

In February 2014, a private company installed 12 CCTV monitoring (24-hour monitoring) outside and inside a family residential building. The information about the CCTV monitoring was clear and transparent and the majority of the residents (18 of 23) had approved this CCTV monitoring. The Supreme Court in a decision dated 29 March 2016 examined the 12 CCTV monitoring installations in order to assess their conformity with the Data Protection Act. The Court held that the interest to the prevention of burglary and act of vandalism in principle overrides the interest of the resident to move at any time inside the residential building. However, the collection of data that enable to assess the private life of the resident is prohibited. Thus, the location of a CCTV monitoring in the main entrance of a family residential building which enables the collection of information about the resident's behaviour, in particular its entry and exit time as well as the persons accompanying the resident is not admissible. The same rule applies to CCTV monitoring installed in front of the laundry room. The Court concluded that the weight of interest between the private and public interest was respected and confirmed the obligation to remove three of the 12 CCTV monitoring installations.

In October 2016, the European Court of Human Rights condemned Switzerland for a violation of Article 8 (right to respect for private and family life) of the European Convention on Human Rights. The Claimant had been involved in a road traffic accident, and subsequently requested a disability pension. Following a dispute with her insurer on the amount of disability pension and years of litigation later, her insurer requested that she undergo a fresh medical examination, in order to establish additional evidence about her condition. When she refused, the insurer hired private investigators to conduct secret surveillance of her. The evidence that they obtained was used in subsequent court proceedings, which resulted in a reduction of the Claimant's benefits. She complained that the surveillance had been in breach of her right to respect for private life, and that it should not have been admitted in the proceedings. The Court held that the insurer's actions engaged state liability under the Convention, since the respondent insurance company was regarded as a public authority under Swiss law. It also held that the secret surveillance ordered had interfered with the Claimant's private life, even though it had been carried out in public places, since the investigators had collected and stored data in a systematic way and had used it for a specific purpose. Furthermore, the surveillance had not been prescribed by law, since provisions of Swiss law on which it had been based were insufficiently precise. In particular, they had failed to regulate with clarity when and for how long surveillance could be conducted, and how data obtained by surveillance should be stored and accessed. There had therefore been a violation of Article 8.

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

The following hot topics are:

- US/Switzerland 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).
- Cloud Computing.

After the European Commission adopted the EU-U.S. Privacy Shield, Switzerland entered into negotiations in order to enter into a similar agreement. On January 2017, the Swiss Federal Council communicated that Switzerland adopted the Swiss-U.S. Privacy Shield. The self-certify to the Swiss-U.S. Privacy Shield should start as from 12 April 2017.

In December 2016, the preliminary draft of the complete revision of the Swiss Federal Act on Data Protection has been submitted for consultation. 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 in order to facilitate continued transborder data flows. Companies will be obliged to take steps to prevent potential data breaches whenever personal data are processed.

Michèle Burnier
Pestalozzi Attorneys at Law Ltd.
Cours de Rive 13
1204 Geneva
Switzerland

Tel: +41 22 999 96 00
Fax: +41 22 999 96 01
Email: michele.burnier@pestalozzilaw.com
URL: www.pestalozzilaw.com

Michèle Burnier graduated from the University of Lausanne and was admitted to the bar in 1994. Thereafter, she worked for a consumer organisation based in Romandie. She subsequently worked for the Swiss Federal Institute of Intellectual Property, where she was attached to the Trademark Department before taking on specific tasks in connection with WIPO. Before she joined Pestalozzi, she worked for several years in another Geneva business law firm. She is regularly quoted by *Chambers*.

In 2017, she became a partner of Pestalozzi. Michèle's areas of expertise are intellectual property, unfair competition, data protection, advertising and e-commerce law, IT and telecommunication, as well as administrative and contract law.

She is a member of various national and international organisations, such as INTA, ASA, LIDC, AROPI and LES (a 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).

Lorenza Ferrari Hofer
Pestalozzi Attorneys at Law Ltd.
Loewenstrasse 1
8001 Zurich
Switzerland

Tel: +41 44 217 92 57
Fax: +41 44 217 92 17
Email: lorenza.ferrari@pestalozzilaw.com
URL: www.pestalozzilaw.com

Lorenza Ferrari Hofer is head of Pestalozzi's IP & TMT practice group and co-head of the Life Sciences Group. Her fields of expertise include intellectual property, unfair competition, data protection and contract law. She has years of experience in the development, licensing, trade and distribution of technology, as well as of therapeutic, health and food products. Lorenza Ferrari Hofer deals with both commercial and litigious matters.

She regularly lectures and publishes in the fields of international licensing and technology transfer, also in relation with big data issues, and in several areas of unfair competition and intellectual property law. Lorenza Ferrari Hofer is a member of various national and international organisations, such as AIPPI (president of the Swiss national group), IBA, INTA, INGRES, and LES. She is consistently recommended by the leading directories of the legal profession such as *The Legal 500 Chambers Europe*, *Who's Who Legal* and *IAM*. Lorenza Ferrari Hofer graduated from the University of Basle (*Dr. iur.* 1993) and was admitted to the bar in 1995. In 2005, she qualified as a solicitor of England and Wales. Lorenza Ferrari Hofer began her professional career at the Swiss Federal Institute of Intellectual Property, where she worked in the Trademark Department before taking on specific tasks in connection with WTO Law (TRIPs Agreement) and UN Law. She subsequently worked for several years as an in-house lawyer for a major Swiss watch and micromechanics manufacturer. Her professional languages are German, Italian, English and French.

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
- 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
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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 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