



ICLG

The International Comparative Legal Guide to:

Data Protection 2014

1st Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

BANNING

Barrera, Siqueiros y Torres Landa, S.C.

CMS Reich-Rohrwig Hainz

Dittmar & Indrenius

DLA Piper

ECIJA ABOGADOS

Eversheds

Gilbert + Tobin Lawyers

Herbst Kinsky Rechtsanwälte GmbH

Hunton & Williams

KALO & ASSOCIATES

Koep & Partners

Marrugo Rivera & Asociados, Estudio Jurídico

Matheson

Mori Hamada & Matsumoto

Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados

Osler, Hoskin & Harcourt LLP

Pachiu & Associates

Pestalozzi

Portolano Cavallo Studio Legale

Raja, Darryl & Loh

Subramaniam & Associates (SNA)

Wigley & Company

Wikborg, Rein & Co. Advokatfirma DA

GLG

Global Legal Group

Contributing Editor

Bridget Treacy,
Hunton & Williams

Account Managers

Edmond Atta, Beth Bassett, Antony Dine, Susan Glinska, Dror Levy, Maria Lopez, Florjan Osmani, Paul Regan, Gordon Sambrooks, Oliver Smith, Rory Smith

Sales Support Manager

Toni Wyatt

Sub Editors

Nicholas Catlin
Amy Hirst

Editors

Beatriz Arroyo
Gemma Bridge

Senior Editor

Suzie Kidd

Global Head of Sales

Simon Lemos

Group Consulting Editor

Alan Falach

Group Publisher

Richard Firth

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 2014

Copyright © 2014

Global Legal Group Ltd.
All rights reserved
No photocopying

ISBN 978-1-908070-98-2

ISSN 2054-3786

Strategic Partners



General Chapter:

1	Data Protection – a Key Business Risk – Bridget Treacy, Hunton & Williams	1
---	--	---

Country Question and Answer Chapters:

2	Albania	KALO & ASSOCIATES: Eni Kalo	7
3	Australia	Gilbert + Tobin Lawyers: Peter Leonard & Ewan Scobie	15
4	Austria	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	24
5	Belgium	Hunton & Williams: Wim Nauwelaerts & Laura De Boel	34
6	Brazil	Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados: Renato Opice Blum	42
7	Canada	Osler, Hoskin & Harcourt LLP: Adam Kardash & Bridget McIlveen	49
8	China	Hunton & Williams LLP Beijing Representative Office: Manuel E. Maisog & Zhang Wei	57
9	Colombia	Marrugo Rivera & Asociados, Estudio Juridico: Ivan Dario Marrugo Jimenez	63
10	Finland	Dittmar & Indrenius: Jukka Lång & Iris Keino	69
11	France	Hunton & Williams: Claire François	77
12	Germany	Hunton & Williams: Dr. Jörg Hladjk & Johannes Jördens	85
13	India	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	94
14	Ireland	Matheson: John O'Connor & Anne-Marie Bohan	105
15	Italy	Portolano Cavallo Studio Legale: Laura Liguori & Federica De Santis	115
16	Japan	Mori Hamada & Matsumoto: Akira Marumo & Hiromi Hayashi	123
17	Kosovo	KALO & ASSOCIATES: Loriana Robo & Atdhe Dika	132
18	Malaysia	Raja, Darryl & Loh: Tong Lai Ling & Roland Richard Kual	140
19	Mexico	Barrera, Siqueiros y Torres Landa, S.C.: Mario Jorge Yanez V. & Federico de Noriega O.	149
20	Namibia	Koep & Partners: Hugo Meyer van den Berg & Chastin Bassingthwaighte	157
21	Netherlands	BANNING: Monique Hennekens & Chantal Grouls	163
22	New Zealand	Wigley & Company: Michael Wigley	175
23	Norway	Wikborg, Rein & Co. Advokatfirma DA: Dr. Rolf Riisnæs & Dr. Emily M. Weitzenboeck	181
24	Romania	Pachiu & Associates: Mihaela Cracea & Ioana Iovanesc	191
25	Slovenia	CMS Reich-Rohrwig Hainz: Luka Fabiani & Ela Omersa	200
26	South Africa	Eversheds: Tanya Waksman	210
27	Spain	ECIJA ABOGADOS: Carlos Pérez Sanz	217
28	Switzerland	Pestalozzi: Clara-Ann Gordon & Dr. Michael Reinle	226
29	United Kingdom	Hunton & Williams: Bridget Treacy & Naomi McBride	234
30	USA	DLA Piper: Jim Halpert & Kate Lucente	242

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

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

EDITORIAL

Welcome to the first edition of *The International Comparative Legal Guide to: Data Protection*.

This guide provides the international practitioner and in-house counsel with a comprehensive worldwide legal analysis of the laws and regulations of data protection.

It is divided into two main sections:

One general chapter entitled *Data Protection – a Key Business Risk*.

Country question and answer chapters. These provide a broad overview of common issues in data protection laws and regulations in 29 jurisdictions.

All chapters are written by leading data protection lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editor Bridget Treacy of Hunton & Williams for her invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.co.uk.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

Switzerland

Clara-Ann Gordon



Pestalozzi

Dr. Michael Reinle



1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Federal Act on Data Protection as of 19 June 1992 (Data Protection Act, hereinafter “DPA”). As Switzerland is not a member of the EU, it does not have to comply with the EU Data Protection Directive or any other directives applicable in this field of expertise.

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

Any 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 like the patient secrecy regarding health data as set out in article 321 of the Swiss Criminal Code have an impact when respective data is processed.

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

The Federal Data Protection and Information Officer (“FDPIC”) is the relevant authority. The Cantonal Data Protection and Information Officer 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 (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 the 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 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).
- **“Data Subject”**
Natural or legal persons whose data is processed (see article 3 lit. b 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.
- **“Direct Personal Data”**
DPA does not differentiate between direct personal data and indirect personal data.
- **“Indirect Personal Data”**
DPA does not differentiate between direct personal data and indirect personal data.
- **Other key definitions**
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 is accessible by 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 regulation.

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).

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 is transferred to a country that has no appropriate 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). FDPIC must be informed about these safeguards (see article 6 para. 3 DPA). 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 in any case (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 (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 answers to question 5.1 above.

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.)

The data controller who transfers personal data pursuant to the DPA abroad (see definition in answer to question 2.1 above); the controller of the data files (see definition in answer to question 2.1 above).

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.)

Regarding the information in connection with cross-border transfers: no detailed information is required if the standard contractual clauses of the EU or the FDPIC are used. Otherwise, the respective contract clauses must be disclosed to the FDPIC.

Regarding the registration of 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.

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

On complaint, the respective entities or individuals may be fined if they did not comply wilfully (see article 34 para. 2 DPA). The fine can be up to 10,000.00 Swiss francs.

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 current information changes. There is, however, no strict deadline.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

There is no such obligation.

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?

It 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 any more (see article 11a para. 5 DPA).

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

Independence (performs its 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 Ordinance to the DPA).

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 Ordinance to the DPA).

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 Ordinance to the DPA).

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, 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 post and telephone article 3 lit. u of the Unfair Competition Act prohibits to send such communication if the recipient declared in the official telephone registry or directly at the mail box that he does not wish to receive such communication.

Article 3 lit. o of the Unfair Competition Act requires regarding emails and SMS text messages that such communication may only be sent with the prior consent of the recipients and with the information relating to 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?

No, they are not.

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

On complaint, the respective entity may be sanctioned in case of intentional conduct with prison for up to three years or a monetary penalty of up to 1,080,000.00 Swiss francs (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 conduct.

7.4 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 about opt-out mechanisms (see article 45c of the Swiss Telecommunication Act).

7.5 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.

7.6 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 actions as the main regulation regarding cookies is not in the DPA.

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

A fine not exceeding 5,000.00 Swiss francs (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 transborder disclosure means any provision 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 appropriate 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.

This assumption 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 on the general grounds for justification (according to Article 13 DPA) is not available.

It can be stated as a rule of thumb that all those countries, which have either ratified the ETS 1082 agreement or have implemented the EU directive on data protection comply with Swiss legislation.

In addition, the FDPIC has prepared a non-binding list of those countries whose data protection legislation should ensure appropriate protection.

However, those who want to be sure that the publication of personal data abroad is compatible with Swiss data protection laws, should always take additional precautions according to Article 6 para. 2 DPA.

The disclosure of data abroad within a group of companies is also permissible in countries without adequate legislation, if the companies concerned are subject to data protection regulations which ensure appropriate protection. This regulation privileges international data transfer within a group of companies (Article 6 para. 2 lit. g DPA).

Data protection regulations which ensure appropriate protection must at least contain the elements recommended by the FDPIC for international data transfer, namely:

- listing of purposes of use split according to data categories;
- binding agreement on disclosing data for indicated purposes only;

- protection of the rights of the persons concerned (in particular rights to information and rectification);
- 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 is both, inadequate legislation in the recipient country as well as insufficient data protection regulations, international data transfer among affiliated companies in the group is still permitted, provided one of the minimum requirements of Article 6 para. 2 lit. a to f DPA is satisfied:

- sufficient guarantees ensure appropriate protection;
 - by the agreement of data protection clauses in contracts or by voluntary adherence to control bodies, such as the “Safe Harbor Privacy Framework”;
- the person concerned has given permission in the individual case and following appropriate information;
- processing is in immediate association with the conclusion or execution of a contract and it concerns personal data of the contracting party;
- disclosure in the individual case is essential for the preservation of an overriding public interest or for the determination, exercise or enforcement of legal claims before the court;
- disclosure is necessary in the individual case in order to protect the life or physical integrity of the person concerned; or
- the person concerned has made the data generally available without explicitly prohibiting its processing.

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 an adequate contractual guarantee (Article 6 para. 2 lit. a DPA) has been concluded or that data protection regulations within the group of companies (Article 6 para. 2 lit. g DPA) have been implemented. As long as the contractual guarantee is in line with the provisions in the EU standard clauses, then the respective data protection agreement does not have to be submitted. Also the group internal policy does not need to be submitted. In both instances it suffices to just inform the FDPIC of the fact that this has happened.

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 whistleblowing as such. Any whistleblowing initiatives must, however, comply with the general requirements of the DPA. There are currently attempts to regulate the prerequisites of justified whistleblowing and the development of a more comprehensive protection of the whistleblower.

Accordingly, the protection of the employee (whistleblower) is very weak. The employee (unfortunately) is exposed to civil (e.g. termination of his/her job) and criminal (e.g. offences due to false allegations, industrial espionage) sanctions. There are also no restrictions as such as to what can be reported on the whistleblowing hotline.

Moreover, there is no duty to notify or register the Helpline with the respective authorities *per se*. However, collections of sensitive personal data must be registered with the respective authorities, even if the persons concerned are aware of the processing. Excluded from this are data collections by companies, which have appointed an internal, but still an independent officer responsible for data protection. Swiss doctrine is mainly of the opinion that companies with whistleblower hotlines do not have to register the respective data collections, because there is usually no sensitive personal data or personality profiles of employees among such data.

Whistleblowing 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 to take care of its employees. The employer generally has to implement all necessary measures in order to ensure that the personality rights of the whistleblower are not infringed. Accordingly, the employee must be informed transparently and comprehensively about all aspects of the whistleblowing hotline (where it is operated, who is operating it, etc.) and the consequences her/his whistleblowing activities can 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.

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 answer to question 9.1 above: there is no requirement for registration/notification of whistleblower hotlines *per se*.

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 requirement to register/notify or obtain prior approval for the use of CCTV.

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

The employee must generally be previously and transparently informed about the type and method of the electronic monitoring, the scope and period of the monitoring and the purpose thereof.

The anonymous monitoring (including monitoring against search strings) of e.g. employees' use of company-provided information

technology in order to check on compliance with e.g. the email and Internet user guide or other policies in force, is permissible.

With regard to pseudonyms (i.e. an abbreviation for an employee known only to a very limited group of persons) only spot checks are permissible.

In both cases the employees need to be informed of the fact that their information technology use can/will be monitored.

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 prerequisites have to be fulfilled: (i) justified suspicion of criminal offence; (ii) monitoring and reading of emails is urgently necessary to confirm or dispel suspicion; (iii) such is necessary for the conservation of evidence; and (iv) there is no overriding interest of the employee. If there is an overriding interest, then the consent of the employee has to be obtained. Please note that any evidence not collected in compliance with the applicable law/rules mentioned above, may possibly 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) are not permitted and infringe the applicable Swiss law. According to the FDPIC this applies to so-called content scanners (if done clandestinely). A content scanner is a piece of 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 answer to question 10.2 above: yes, prior transparent information is required, however no consent is necessary.

10.4 To what extent do work councils/trade unions/employee representatives need to be notified or consulted?

There is no duty to consult work councils/trade unions/employee representatives. However, in practice it is recommended to at least inform them.

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 however no statutory provisions. 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 is processed in the cloud; and the necessary security and organisational measures must be implemented.

Moreover, the FDPIC has issued a guidance which in a nutshell suggests that the cloud provider must be chosen carefully and instructed and monitored accordingly. The appropriate technical and organisational necessities must be implemented, adequate protection must be guaranteed (in particular with data transfers to countries which do not have the same level of data protection). Finally, the right to obtain information and the right to have data deleted or corrected must be respected.

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 security measures will likely be applicable to these kind of providers.

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. Also here the general provisions of the DPA must be complied with. 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 Ordinance to the DPA gives 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 the 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 current state of the article.
- (3) These measures must be reviewed periodically.

Finally, article 9 Ordinance to the DPA states:

- (1) The controller of the data file shall, in particular for the 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 the access to facilities in which personal data is 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 is 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 so that the 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. transparency, 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 answer to question 13.2 above.

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 are being breached, the FDPIC can recommend that the federal body concerned change the method of processing or abandon the processing. He informs the department concerned or the Federal Chancellery of his recommendation. If a recommendation is not complied with or is rejected, he 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.	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 on a regular basis his recommendations and publishes them on his website.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within Switzerland 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 authorities within the international judicial assistance (in civil or criminal matters) system.

And also when such requests are made outside pending proceedings, due to the blocking statutes (e.g. articles 271 and 273 of the Swiss Criminal Code) companies within Switzerland cannot just simply comply with foreign e-discovery requests. 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). In any event the provisions of the DPA have to be complied with: e.g. special measures must be implemented when disclosing personal data to authorities abroad.

15.2 What guidance has the data protection authority(ies) issued?

The FDPIC has issued guidance regarding this subject matter. Basically, the guidance comes to the same conclusions as set out in the answer to question 15.1.



Clara-Ann Gordon

Pestalozzi
Loewenstrasse 1
8001 Zurich
Switzerland

Tel: +41 44 217 92 80
Fax: +41 44 217 92 17
Email: clara-ann.gordon@pestalozzilaw.com
URL: www.pestalozzilaw.com

Clara-Ann Gordon graduated from the University of Berne and was admitted to the Bar in 1997. Thereafter, she attended the University of London, Queen Mary & Westfield College and graduated in 1998 (LL.M. in intellectual property). Before she joined Pestalozzi, she worked for several years in another Zurich business law firm. She is regularly quoted by Chambers, Best Lawyers, Legal500, Who's Who Legal and EuroMoney's Guide to leading Information Technology Lawyers.

In 2009 she became a partner of Pestalozzi. Clara-Ann's areas of expertise are intellectual property, IT, telecommunications and media law. She is a member of various national and international organisations, such as AIJA, AIPPI, ASUT, IBA, INGRES, INTA, ITechlaw and LES. Moreover, she is Co-Chair of the IBA Technology Law Committee and Vice-Chair of the Arbitration, Mediation and Dispute Resolution Committee of ITechLaw. Further she is a member of the INTA Enforcement Committee and an IT mediator/arbitrator with SGOA.



Dr. Michael Reinle

Pestalozzi
Loewenstrasse 1
8001 Zurich
Switzerland

Tel: +41 44 217 92 48
Fax: +41 44 217 92 17
Email: michael.reinle@pestalozzilaw.com
URL: www.pestalozzilaw.com

Michael Reinle's fields of expertise include intellectual property, unfair competition, data protection, and contract law. In addition, he has experience in the areas of food and healthcare law as well as sports law. Michael Reinle deals with both commercial and litigious matters. He publishes in the field of intellectual property law and acts as a speaker in his field of expertise on a regular basis. Furthermore, he is a member of the AIPPI Working Group Q212 regarding general trademark laws.

Michael Reinle graduated from the University of St. Gallen in 2001 (*lic. iur.*) and 2007 (*Dr. iur.*). He was admitted to the Bar in 2004. He earned a degree from the University of Chicago Law School in 2010 (LL.M.). Before rejoining Pestalozzi in 2010 as an associate, he worked as an associate for a law firm, as an academic assistant at the University of St. Gallen and as a junior associate for Pestalozzi.



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 benefit from the know-how of over 150 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 Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet

GLG

Global Legal Group

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

www.iclg.co.uk