The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 2
(published in November 2015 – editor Alan Charles Raul)

For further information please email
Nick.Barette@lbresearch.com

Chapter 24

SWITZERLAND

Jürg Schneider and Monique Sturny[1]

I OVERVIEW

Data protection and data privacy are fundamental constitutional rights protected by the Swiss Constitution. Swiss data protection law is set out in the Swiss Federal Data Protection Act of 19 June 1992 (DPA)[2] and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 14 June 1993 (DPO).[3] As Switzerland is neither a member of the European Union (EU) nor of the European Economic Area (EEA), Switzerland has no general duty to implement or comply with EU laws.[4] Accordingly, Swiss data protection law has some peculiarities that differ from the data protection laws of most EU Member States. However, because of Switzerland's location in the centre of Europe and its close economic relations with the EU Member States, Swiss law is in general strongly influenced by EU law, both in terms of content and interpretation. A closer alignment of Swiss data protection law with the EU data protection provisions is also one of the aims of the currently pending reform of the DPA.

The Swiss Data Protection and Information Commissioner (the Commissioner) is the responsible authority for supervising both private businesses and federal public bodies with respect to data protection matters. The Commissioner has published several explanatory guidelines that increase legal certainty with respect to specific issues such as data transfers abroad, technical and organisational measures, processing of data in the medical sector and processing of employee data.[5] Despite the lack of drastic sanctions in

1 Jürg Schneider is a partner and Monique Sturny is an associate at Walder Wyss Ltd.

2 Classified compilation (SR) 235.1, last amended as of 1 January 2014.

3 Classified compilation (SR) 235.11, last amended as of 1 December 2010.

4 Specific duties exist in certain areas based on international treaties.

5 The guidelines are not legally binding, but do set *de facto* standards.

respect of data protection, it is nonetheless a topic at the forefront of public attention in Switzerland, especially given the active presence of the Commissioner and the high level of media attention given to data protection matters.

II THE YEAR IN REVIEW

There have been a number of noteworthy reforms over the past few months, some of which are still pending and some of which are expected to enter into force shortly.

An evaluation of the DPA initially conducted in 2011 has revealed the need for reform of the DPA. On 1 April 2015, the Swiss Federal Council formally decided to undertake a revision of the DPA. The Swiss Federal Council has instructed the Federal Department of Justice and Police to submit a preliminary draft for a revision of the DPA by the end of August 2016 at the latest. The aim of this reform is to lay the foundations allowing Switzerland to ratify the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and, to the extent this is necessary in the context of further development of the Schengen/Dublin acquis, the adaptation of the DPA to the EU data protection provisions (see Section X, *infra*, for more details).

The Swiss Act on the Supervision of Postal and Telecommunication Services and the Act regarding Intelligence Services are currently under review. The purpose of the proposed amendments is to increase the scope for surveillance of individuals, in particular in connection with the prevention of terrorism. These proposed amendments have been criticised in particular by the Commissioner as undermining privacy and other fundamental rights of data subjects. The reforms were in principle accepted by a majority of both parliamentary chambers in summer 2015. The amended Act on the Supervision of Postal and Telecommunication Services may enter into force in the course of 2016 at the earliest.[6, 7]

A further pending reform concerns the Swiss legislation dealing with the Commercial Register (the register of companies). As part of this particular reform the Swiss parliament has decided that no 'right to be forgotten' shall be introduced with respect to Commercial Register data.

Finally, the Swiss parliament adopted a new law on electronic files for patients in summer 2015, establishing the legal basis for the maintenance of electronic medical files.[8]

6 Commissioner, 22nd Annual Report 2014/2015, p. 8.

7 The amended Act regarding Intelligence Services is not expected to enter into force before 2017.

8 See www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/14832/index.html? lang=de (in German; no English version available; last visited on 14 September 2015).

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

The Swiss Constitution of 18 April 1999[9] guarantees the right to privacy in its Article 13. The federal legislative framework for the protection of personal data mainly consists of the DPA and the DPO.[10] Further relevant data protection provisions are contained in the Federal Ordinance on Data Protection Certification of 28 September 2007.[11] Specific data protection issues such as, *inter alia*, transfers of data abroad, data protection in relation to employees or as regards the medical sector are dealt with in more detail in the respective guidelines published by the Commissioner.[12]

Key definitions under the DPA[13]

a Personal data (or data): all information relating to an identified or identifiable person. Unlike the data protection laws of most other countries, Swiss data protection law protects personal data relating to both individuals and legal entities. Hence, the term 'person' refers not only to natural persons (individuals), but also to legal entities, such as corporations, associations, cooperatives or any other legal entity, as well as partnerships.

b Data subject: an individual or legal entity whose data is being processed.

c Processing of personal data: any operation with personal data, irrespective of the means applied and the procedure, and in particular the storage, use, revision, disclosure, archiving or destruction of data.

d Sensitive personal data: data relating to:
- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or racial origin;
- social security measures; and
- administrative or criminal proceedings and sanctions.

e Personality profile: a collection of data that permits an assessment of essential characteristics of the personality of a natural person. Swiss data protection law provides an enhanced data protection level for personality profiles, similar to the protection of sensitive personal data.

f Data file: any set of personal data that is searchable by data subject.

---

9 Classified compilation (SR) 101, last amended as of 14 June 2015.

10 The federal legislative framework exclusively applies to the processing of personal data by private persons and federal bodies. Processing of personal data by Swiss cantonal bodies is governed by the specific and distinct data protection legislation of each of the 26 cantons. Unless explicitly set forth otherwise, this overview does not address the particularities of the data protection legislation on the cantonal level.

11 Classified compilation (SR) 235.13, last amended as of 1 April 2010.

12 As mentioned above (footnote 5), the guidelines are not legally binding, but do set *de facto* standards.

13 Article 3 DPA.

g Controller of the data file: under Swiss data protection law, the term 'controller' is only used in the sense of 'controller of the data file'. The controller of the data file is the private person or federal body that decides on the purpose and content of a data file.

ii General obligations for data handlers

Anyone processing personal data must observe the following general obligations:[14]

Principle of good faith

Personal data must be processed in good faith. It may not be collected by misrepresentation or deception.

Principle of proportionality

The processing of personal data must be proportionate. This means that the data processing must be necessary for the intended purpose and reasonable in relation to the infringement of privacy. Subject to applicable regulations on the safekeeping of records, personal data must not be retained longer than necessary.

Principle of purpose limitation

Personal data may only be processed for the purpose indicated at the time of collection, unless the purpose is evident from the circumstances or the purpose of processing is provided for by law.

Principle of transparency

The collection of personal data and in particular the purposes of its processing must be evident to the data subject concerned. This principle does not always lead to a specific disclosure obligation, but it will be necessary to give notice of any use of personal data that is not apparent to the data subject from the circumstances. For example, if personal data is collected in the course of concluding or performing a contract, but the recipient of the personal data intends to use the data for purposes outside the scope of the contract or for the benefit of third parties, then such uses of the personal data must be disclosed to the data subject.

Principle of data accuracy

Personal data must be accurate and kept up to date.

Principle of data security

Adequate security measures must be taken against any unauthorised or unlawful processing of personal data and against intentional or accidental loss, damage to or destruction of personal data, technical errors, falsification, theft and unlawful use, unauthorised access, changes, copying or other forms of unauthorised processing. If

14 Article 4, 5 and 7 DPA.

a third party is engaged to process personal data, measures must be taken to ensure that such third party processes the personal data according to the given instructions and that such third party implements the necessary adequate security measures.

Detailed technical security requirements for the processing of personal data are set out in the DPO.

Principle of lawfulness

Personal data must be processed lawfully. This means that the processing of personal data must not violate any Swiss legislative standards, including any normative rules set forth in acts other than the DPA and that directly or indirectly aim at the protection of the personality rights of a data subject.

Processing personal data does not necessarily require a justification

Processing personal data does not per se constitute a breach of the privacy rights of the data subjects concerned. Accordingly, processing only requires a justification if it unlawfully breaches the privacy of the data subjects (Article 12 Paragraph 1 in relation to Article 13 DPA).

In general, no justification for processing personal data is required if the data subjects have made the data generally available and have not expressly restricted the data processing (Article 12 Paragraph 3 DPA). On the other hand, a justification is required particularly if the processing violates one of the general data protection principles of the DPA outlined above, if the personal data is processed against the data subjects' express wish or if sensitive personal data or personality profiles are disclosed to third parties for such third parties' own purposes (Article 12 Paragraph 2 DPA).

If a justification for processing is required, such justification exists if either (1) the data subject has consented to it, (2) Swiss (federal, cantonal and municipal) law provides for it, or (3) there is an overriding private or public interest[15] in the data processing (Article 13 Paragraph 1 DPA).

According to Article 13 Paragraph 2 DPA, an overriding private interest of the data handler shall be considered in particular if he or she:

a processes personal data in direct connection with the conclusion or the performance of a contract and the personal data in question is the data of one of the contractual parties;

b competes for business with, or wants to compete for business with, another person and processes personal data for this purpose without disclosing the data to third parties for such third parties' own purposes;

15 The public interest needs must exist from a Swiss perspective. However, this does not only include Swiss public interests. Supporting foreign concerns – depending on the circumstances – may also qualify as a public interest from a Swiss perspective. This needs to be checked on a case-by-case basis.

c processes data that is neither sensitive personal data nor a personality profile to verify the creditworthiness of another person, and discloses such data to third parties for such third parties' own purposes only if the data is required for the conclusion or the performance of a contract with the data subject;

d processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;

e processes personal data for purposes that are not related to a specific person, in particular research, planning or statistics, and the results are published in a manner that does not permit the identification of the data subjects; and

f collects personal data about a person who is a public figure to the extent that the personal data relates to the role of such person as a public figure.

The fact that a data handler has one of the above-listed interests in processing personal data does not mean per se that the data handler has an overriding interest in processing the personal data. The interest of the data handler in processing the personal data must always be weighed against the interest of the data subject in being protected against an infringement of his or her privacy. Only in situations where the interest of the data handler outweighs the interest of the data subject is the processing of personal data justified by the overriding interest of the data handler.

Consent

Processing of personal data does not require consent of the data subject concerned in all instances. However, as mentioned above, consent of the data subject may constitute a possible justification for data processing that would otherwise be unlawful (e.g., because of an infringement of the principles outlined above or in the event of a disclosure of sensitive personal data or personality profiles to third parties for such third parties' own purposes).[16] To the extent that the legality of data processing is based on the consent of the data subject concerned, such consent is only valid if given voluntarily upon provision of adequate information. In the case of processing sensitive personal data or personality profiles, such consent must be given expressly (Article 4 Paragraph 5 DPA).

Registration

Controllers of data files that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties (including affiliates) must register their data files with the Commissioner before they start processing such data (Article 11a DPA). The Commissioner maintains a register of data files that have been registered in this manner that is accessible online. If a controller is required to register, it becomes subject to additional documentary obligations. There are several exceptions to the duty to register data files. *Inter alia*, no registration is required if the controller of the data file (1) is obliged by Swiss law to process the data in question, (e.g., in the case of an employer processing employee data for Swiss social security purposes), or (2) has

16 Cf. Article 12 Paragraph 2 Letter (c) DPA.

nominated its own independent data protection officer monitoring the data protection compliance of the data controller. Several further exceptions are set forth in Article 11a Paragraph 5 DPA and Article 4 Paragraph 1 DPO.

iii Technological innovation and privacy law

Automated profiling and data mining

The legality of automated profiling and data mining is doubtful under Swiss data protection law, as such practices inherently involve the use of personal data for a range of purposes, some of which may not have been disclosed when the personal data was collected. Hence, such practices may constitute an unlawful breach of privacy because of an infringement of the principles of transparency, purpose limitation and proportionality unless justified by law, an overriding public or private interest or consent.

Cloud computing

Cloud computing raises various data protection issues. The Commissioner has issued a guide pointing out the risks and setting out the data protection requirements when using cloud computing services.[17]

In particular, the processing of personal data may only be assigned to a cloud service provider if such an assignment is based on an agreement or on the law, if the personal data is processed by the cloud service provider only in the manner permitted for the assignor and if such an assignment is not prohibited by a statutory or contractual duty of confidentiality (Article 10a Paragraph 1 DPA). Furthermore, the assignor must ensure that the cloud service provider guarantees data security (Article 10a Paragraph 2 DPA). The assignor must in particular ensure that the cloud service provider ensures confidentiality, availability and integrity of the personal data by taking adequate measures against unauthorised processing through adequate technical and organisational measures (see Article 7 DPA and Article 8 et seq. DPO). Additionally, if cloud computing services involve disclosures of personal data abroad, the specific requirements for transborder data flows must be complied with (see Section IV, *infra*). Finally, the assignor must also ensure that despite the use of a cloud service provider the data subjects may still exercise their right to information (Article 8 DPA) and may demand deletion or correction of data in accordance with Article 5 DPA.

Big data

From an economic point of view, big data has great potential. In particular, big data offers new opportunities for social or scientific research. However, big data may threaten privacy if the processed data is not or is inadequately anonymised. In fact, the DPA is not applicable to fully and completely anonymised data. However, if the processing of big data involves the processing of data that has not been fully and completely anonymised (for example, because it can be 'de-anoymised' at a later stage by merging

17 Commissioner, 'Guide to cloud computing', available at: www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de (status 2014; last visited on 14 September 2015).

different data files), the right to privacy and the protection of personal data need to be guaranteed. The use of big data that is not entirely anonymised and the general data protection principles of the DPA are potentially conflicting, particularly with regard to the principles of purpose limitation, proportionality and transparency (see Section III.ii, *supra*). Currently, the Commissioner is demanding a fundamental review of the DPA to be able to tackle privacy issues in connection with big data more adequately.[18]

Cookies

Since 2007, the use of cookies has been regulated in Article 45c Letter (b) of the Telecommunications Act of 30 April 1997 (TCA).[19] According to this article, website operators have to inform users about the use of cookies and its purpose. Furthermore, they need to explain how cookies can be rejected (i.e., how cookies can be deactivated in the user's browser). Switzerland basically follows the opt-out principle.

Drones

Drones are becoming smaller, cheaper and easier to operate as technology advances. They are, therefore, being used more and more frequently for private and commercial purposes. In Switzerland, in general, drones of up to 30 kilograms do not require a specific permit, as long as they do not overfly crowds of people and provided that the 'pilot' has visual contact with the drone at all times.[20] Nowadays drones are usually equipped with cameras. As a result, people using drones need to comply with data protection regulations as soon as they view or record identified or identifiable persons. To the extent that such viewing or recording constitutes an unlawful breach of the privacy of the data subjects concerned, it needs to be justified either by the consent of the injured party, by an overriding private or public interest or by law (Article 13 Paragraph 1 DPA).[21]

18 Commissioner, 'Explanatory notes on Big Data', available at: www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de (status 2014; last visited on 14 September 2015).

19 Classified compilation (SR) 784.10, last amended as of 1 July 2010.

20 Ordinance of the Federal Department of the Environment, Transport, Energy and Communications (DETEC) on special categories of aircraft of 24 November 1994, last amended as of 15 July 2015, classified compilation (SR) 748.941.

21 It must further be noted that, according to Article 179 quater CC, a person who, without consent, observes with a recording device or records with an image-carrying device information from the secret domain of another person or information from the private domain of another person that is not readily available to everyone is criminally liable; see also Commissioner, 'Video surveillance with drones by private persons', available at: www.edoeb.admin.ch/datenschutz/00625/00729/01171/index.html?lang=de (status 2014; in German; no English version available; last visited on 14 September 2015).

iv Specific regulatory areas

Processing of employee data in general

Article 328b of the Swiss Code of Obligation (CO) applies in addition to the DPA to the processing of personal data of employees.

According to Article 328b CO, the employer may process personal data concerning an employee only to the extent that such personal data concerns the employee's suitability for his or her job or is necessary for the performance of the employment contract. Article 328b CO is mandatory, and any deviation from this provision to the disadvantage of the employee is null and void (Article 362 CO).[22]

Furthermore, Article 26 of Ordinance 3 to the Employment Act[23] prohibits the use of systems that monitor the behaviour of employees, except if such monitoring systems are necessary for other legitimate reasons (e.g., quality control, security requirements, technical reasons, etc.) and provided that such systems do not impair the health and mobility of the employees concerned. If monitoring is required for legitimate reasons, it must at all times remain proportionate (i.e., limited to the extent absolutely required) and the employees must be informed in advance about the use of monitoring systems. Permanent monitoring is in general not permitted.

The Commissioner has issued specific guidelines with respect to the processing of employee data.[24]

Monitoring of internet and email use by employees

As regards monitoring of internet and email use by employees in particular, the following requirements apply: (1) the employer shall issue a 'use policy' that describes the permitted uses the employee may make of company internet and email resources, (2) constant individual analysis of log files is not allowed, (3) permanent anonymous analysis of log files and random pseudonymised analysis are admissible to verify whether the use policy is complied with, (4) individual analysis of log files is only allowed if the employee has been informed in advance of this possibility (e.g., in a 'monitoring policy') and if misuse has been detected or there is a strong suspicion of misuse, and (5) the monitoring policy must particularly indicate the possibility of an individual analysis, the possibility of forwarding such an analysis to the HR department in the event of misuse and any possible sanctions. As a general rule, employers shall not read any employee emails that have private content (even if misuse has been established). In the event of specific suspicion of a criminal offence, evidence may, however, be saved and the employer may refer to the criminal prosecution authorities for further prosecution.

---

22 Some legal authors, however, hold that an employee may specifically and unilaterally consent (i.e., not in the employment contract or in any other agreement with the employer) to the processing of personal data that goes beyond Article 328b CO.

23 Ordinance 3 to the Employment Act (health care) of 18 August 1993, last amended as of 1 May 2010, classified compilation (SR) 822.113.

24 Commissioner, 'Guide on the processing of personal data in the work area' (status October 2014; www.edoeb.admin.ch/datenschutz/00628/00629/00633/index.html?lang=de, in German; no English version available; last visited on 14 September 2015).

Whistle-blowing hotlines

The use of whistle-blowing hotlines is not specifically regulated by the DPA and the CO.[25] Hence, the general rules, in particular on data and employee protection, apply. In a nutshell, whistle-blowing hotlines can be used if certain minimum requirements are met, such as, *inter alia*: (1) the transparent informing of employees, contractors, etc. about the existence of the whistle-blowing hotline; (2) the informing of relevant employees, contractors, etc. of allegations about them contained in a specific whistle-blowing report, unless there is an overriding interest not to do so to protect the ensuing investigations or the reporting person; (3) adequate safeguards to protect the data subjects from false or slanderous accusations; and (4) strong state-of-the-art security measures. It is important to verify compliance on an individual basis before implementing a whistle-blowing hotline. In particular and unless an exception applies, whistle-blowing hotlines (and the underlying data files, respectively) may require prior registration with the Commissioner (see Section III.ii, *supra*), and in the event of transfers abroad, specific requirements must be met (see Section IV, *infra*).

Bring your own device (BYOD)

Using BYOD causes data protection concerns because of the difficulty in separating private and business data. The Commissioner recommends respecting the following rules while using BYOD: (1) establish clear use regulations about what is allowed and what is prohibited, (2) maintain a separation of business and private data (both technical and logical), (3) ensure data security (e.g., through encryption or passwords), (4) establish clear regulations on where the business data is stored, (5) use of employees' own devices must be approved in advance by a person responsible within the company, and (6) establish clear regulations regarding access to the device by the employer.[26]

IV INTERNATIONAL DATA TRANSFER

Any disclosure of personal data from Switzerland to countries abroad must comply with the DPA. A disclosure of data abroad occurs when personal data is transferred from Switzerland to a country outside Switzerland or when personal data located in Switzerland is accessed from outside Switzerland. The DPA prohibits a disclosure of personal data abroad if such a transfer could seriously endanger the personality rights of

25 The Swiss Federal Council has submitted a proposal for a specific regulation with respect to whistle-blowing to the Swiss federal parliament. This proposal was, however, rejected by both chambers of the parliament (cf. press release of the Swiss federal parliament dated 10 September 2015; available at: www.parlament.ch/d/sessionen/sda-sessionen/Seiten/20150910_bsd042_ Whistleblower.aspx; in German, not available in English; last visited on 14 September 2015). It is uncertain when the Swiss Federal Council will submit a revised proposal.

26 Commissioner, 'Bring Your Own Device (BYOD)' (available at: www.edoeb.admin.ch/datenschutz/00763/01249/index.html?lang=de; in German; no English version available; last visited on 14 September 2015).

the data subjects concerned. Such a danger may in particular occur if the personal data is disclosed to a country whose legislation does not guarantee an adequate protection for personal data.

The Commissioner has published a (non-binding) list of countries that provide an adequate data protection level with respect to individuals.[27] As a rule, the countries that have implemented EU Directive 95/46/EC are considered to provide an adequate data protection level relating to individuals. However, according to the aforementioned list, most of these countries do not provide an adequate data protection level with respect to data relating to legal entities.

With respect to data transfers to non-EU or non-EEA countries, it is necessary to check on a case-by-case basis whether such a country provides an adequate level of data protection with respect to personal data pertaining to individuals and legal entities.[28] The same applies for transfers of personal data relating to legal entities to EU or EEA countries.[29]

If personal data is to be transferred to a country that does not provide an adequate data protection level for the personal data being transferred, such a transfer may only occur if (Article 6 Paragraph 2 DPA):

a sufficient safeguards, in particular contractual clauses (typically EU Model Contract Clauses adapted to Swiss law requirements), ensure an adequate level of protection abroad;

b the data subject has consented in an individual specific case;

c the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;

27 See list of countries: www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang =de (in German; no English version available; last visited on 14 September 2015).

28 Following the decision of the Court of Justice of the European Union of 6 October 2015 (Judgment C-362/14) declaring that the US-EU Safe Harbor Framework is invalid, the Commissioner issued a statement on 22 October 2015, according to which he no longer considers the US-Swiss Safe Harbor Framework as a sufficient legal basis for the transfer of personal data from Switzerland to the United States. The Commissioner recommends, *inter alia*, entering into contractual safeguards (i.e., data transfer agreements) in the sense of Article 6 Paragraph 2 DPA and requests that companies make the necessary contractual amendments until the end of January 2016 (cf. http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html; in German; no English version available; last visited on 26 October 2015).

29 It can, in our view, be reasonably argued that the fact that most EU or EEA member countries' data protection legislation does not specifically protect personal data pertaining to legal entities does not per se result in an absence of adequate protection. The protection for such data may also be adequate based on other legislation. Furthermore, the transfer of personal data pertaining to legal entities does not necessarily seriously endanger the personality rights.

d disclosure is essential in the specific case to either safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;

e disclosure is required in the specific case to protect the life or the physical integrity of the data subject;

f the data subject has made the data generally accessible and has not expressly prohibited its processing;

g disclosure is made within the same company or the same group of companies, provided those involved are subject to data protection rules that ensure an adequate level of protection (i.e., that have adopted binding corporate rules (BCRs)).

In addition, in the case of the exceptions mentioned under (a) and (g) above, the Commissioner must be informed in advance (i.e., before the transfer takes place) about the safeguards that have been taken or the BCRs that have been adopted. If the safeguards consist of EU Model Contract Clauses adapted to Swiss law requirements or other contractual clauses explicitly accepted by the Commissioner,[30] then it is sufficient to inform the Commissioner that such clauses have been entered into, and there is no need to actually submit the clauses to the Commissioner for review. As regards information about BCRs, it is common practice to submit a copy of such rules to the Commissioner (including, if applicable, a copy of a letter of the coordinating EU Member State's data protection authority authorising the BCRs on an EU level).

V COMPANY POLICIES AND PRACTICES

According to Article 11 Paragraph 1 DPA, the private controller[31] of an automated data file subject to registration under Article 11a Paragraph 3 DPA that is not exempted from the registration requirement under Article 11a Paragraph 5 Letters (b)–(d) DPA shall issue a processing policy that describes in particular the internal organisation, data processing and control procedures and contains documentation on the planning, realisation and operation of the data file and the information technology used. This policy must be updated regularly and made available upon request to the Commissioner.

Other than in the aforementioned case, the DPA does not explicitly require private personal data handlers to put in place any specific policies as regards the processing of personal data. However, for private personal data handlers to effectively ensure compliance with material and formal data protection requirements, it has become

30 Cf. the standard contractual clauses for the transborder outsourcing of data processing accepted by the Commissioner, available at: www.edoeb.admin.ch/datenschutz/00626/00753/00969/index.html?lang=en (status November 2013; last visited on 14 September 2015).

31 Federal public controllers of data files have a similar obligation to issue a processing policy for automated data files that contain sensitive personal data or personality files, are used by two or more federal bodies, are disclosed to third parties or are connected to other data files (see Article 21 DPO).

best practice for large and medium-sized companies to adopt and implement various policies in this area. In particular, the following policies (either in separate or combined documents) are recommended:

a a policy regarding processing of job applicant and employee personal data (including a policy that governs the use by employees of the company's information technology resources, monitoring by the employer of employees' use of such resources and possible sanctions in the event of misuse, rules on BYOD, etc.);

b a policy regarding processing of customer personal data;

c a policy regarding processing of supplier personal data;

d a whistle-blowing policy;

e a policy or privacy notices for collecting and processing personal data on a company's websites;

f a policy on data and information security (qualification of data according to risk, required measures per risk category, access rights, procedures in the event of data breaches, internal competence, etc.); and

g a policy on archiving of personal data and record-keeping (including guidelines on how long different categories of data must be stored).

Contrary to other countries' legislation, the DPA does not require private data handlers to appoint an internal data protection officer. For this reason, and until a few years ago, companies' internal data protection officers have not played a very important role in Switzerland compared with their role in other countries. However, in the past few years, more and more medium-sized and large companies domiciled in Switzerland have chosen to appoint internal data protection officers. In fact, appointing an internal data protection officer is one way for private data controllers to avoid having to register data files with the Commissioner that otherwise would have to be registered (see Article 11a Paragraph 3 DPA in relation to Article 11a Paragraph 5 Letter (e) DPA; see also Section III.ii, *supra*). Currently, approximately 250 companies have notified the Commissioner of their appointment of internal data protection officers.

BCRs ensuring an adequate level of protection of personal data on a group-wide level facilitate the cross-border disclosure of personal data among group companies (see Section IV, *supra*). Despite this fact, and until recently, BCRs have not played a very important practical role in Switzerland. In the past few years, there has, however, been a noticeable increase in the number of large companies adopting BCRs and informing the Commissioner accordingly. We expect this number to further increase in the next few years.

VI DISCOVERY AND DISCLOSURE

In Switzerland, the taking of evidence constitutes a judicial sovereign function of the courts rather than of the parties. Therefore, taking evidence in a foreign state court and in regulatory proceedings constitutes an act of a foreign state. Such acts, if they take place in Switzerland, violate Swiss sovereignty and are prohibited by Article 271 of the

Swiss Criminal Code of 21 December 1937 (CC),[32] unless they are authorised by the appropriate Swiss authorities by way of judicial assistance. A violation of Article 271 CC is sanctioned with imprisonment of up to three years or a fine of up to 1.08 million Swiss francs. It is important to note that transferring evidence outside Switzerland for purposes of complying with a foreign country's order such as a foreign court order does not prevent an application of Article 271 CC. Moreover, Switzerland does not accept a voluntary production of evidence even if foreign procedural laws require such a production. Therefore, evidence may only be handed over to foreign authorities lawfully by following mutual legal assistance proceedings. If one is requested to produce evidence in a foreign court or in regulatory proceedings, by way of pending mutual legal assistance proceedings, the DPA does not apply to such a production (Article 2 Paragraph 2 Letter (c) DPA).[33] As a consequence and in particular, evidence containing personal data may in such case be disclosed abroad to foreign parties or authorities located in countries without adequate protection of personal data without having to comply with the restrictions set forth in Article 6 DPA.[34]

In addition to Article 271 CC, Article 273 CC prohibits industrial espionage of manufacturing and business secrets by foreign official agencies, foreign organisations, foreign private enterprises, or their agents. Accordingly, manufacturing and business secrets with sufficient connection to Switzerland may only be released or communicated abroad when (1) the owner of the secret relinquishes its intent to keep the information secret, (2) the owner of the secret agrees to disclose this information, (3) all third parties consent to such a disclosure, (4) Switzerland has no immediate, sovereign interest in keeping the information secret, and (5) all requirements set forth by the DPA (in particular as regards cross-border transfers) are complied with. However, Article 273 CC does not apply in cases in which Swiss authorities have granted judicial assistance and disclosure takes place in accordance with such proceedings.

32 Classified compilation (SR) 311.0, last amended as of 1 January 2015.

33 The DPA does also not apply to pending Swiss civil proceedings, pending Swiss criminal proceedings and pending Swiss proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance (see Article 2 Paragraph 2 Letter (c) DPA).

34 In contrast, producing and taking evidence in purely private foreign arbitral proceedings is not subject to Article 271 CC and therefore does not require that the parties follow the requirements of mutual assistance proceedings. However, as the DPA fully applies to the processing of personal data in foreign-based private arbitral proceedings, any cross-border disclosure must comply with the requirements set forth in Article 6 DPA (see Section IV, *supra*). For more details and exceptions, see Jürg Schneider, Ueli Sommer, Michael Cartier, in: Catrien Noorda, Stefan Hanloser (eds), *E-Discovery and Data Privacy: A Practical Guide*, Kluwer Law International BV, 2011, Chapter 5.25, Switzerland.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner supervises compliance of both federal bodies and private persons (individuals and legal entities) with the DPA, DPO and other federal data protection regulations.[35] The Commissioner fulfils these tasks independently without being subject to the directives of any authority.

For this purpose, the Commissioner may investigate cases either on his or her own initiative or at the request of a third party. The Commissioner may request the production of files, obtain information and request that a specific instance of data processing is demonstrated to him or her. If such an investigation reveals that data protection regulations are being breached, the Commissioner may make recommendations as to how the method of data processing shall be changed or that the data processing activity shall be stopped. If such a recommendation is not complied with, the Commissioner may initiate proceedings leading to a formal decision on the matter.

In the case of recommendations to federal bodies, the Commissioner may refer the case to the competent department or the Swiss Federal Chancellery for a formal decision. Both the Commissioner and any persons concerned by such a decision may file an appeal against such a decision with the Swiss Federal Administrative Court. The appeal decision can be appealed to the Swiss Federal Supreme Court.

In the case of recommendations to private persons, the Commissioner may refer the case to the Swiss Federal Administrative Court for a decision. Both the Commissioner and the addressee of such a decision may file an appeal against such a decision with the Swiss Federal Supreme Court.

The Commissioner does not have the power to issue any fines. However, based on Article 34 DPA the competent criminal judge may, upon complaint, sanction private persons with a fine of up to 10,000 Swiss francs if they have wilfully breached their obligations to (1) provide information upon request of the data subject concerned under Article 8 DPA; (2) provide information on the collection of sensitive personal data and personality profiles under Article 14 DPA; (3) inform the Commissioner about the safeguards and data protection rules in relation to a transfer of personal data abroad under Article 6 Paragraph 3 DPA; (4) register a database with the Commissioner; or (5) cooperate with the Commissioner (Article 34 DPA). Furthermore, anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality

35 The processing of personal data by cantonal and communal bodies is regulated by cantonal law (see footnote 10). Each canton has a cantonal data protection authority, be it a cantonal data protection officer or a commission competent for cantonal and communal data protection matters. Some cantons have jointly appointed an inter-cantonal data protection authority.

profiles that have come to his or her knowledge in the course of his or her professional activities is, upon complaint, liable to a fine of up to 10,000 Swiss francs (Article 35 DPA in connection with Article 106 Paragraph 1 of the CC).[36]

ii Recent enforcement cases

The Swiss Federal Supreme Court's decision of 12 January 2015 in connection with the tax dispute between certain Swiss banks and the United States is particularly noteworthy. Based on the right of access set forth in Article 8 DPA, the court obliged a Swiss bank to provide its employees with copies of all documents transferred to the US Department of Justice in April 2012 containing their personal data.[37]

As regards the processing of employee personal data, the Swiss Federal Supreme Court held in 2013 that the monitoring of an employee's use of email and internet that lasted for three months and included taking regular screenshots was illegal and not proportionate. Moreover, the monitoring was not backed by an internal policy that permitted monitoring under specific, transparently disclosed circumstances.[38]

Finally, another noteworthy but somewhat older decision of the Swiss Federal Supreme Court concerns Google's street mapping services 'Street View'. In its decision of 2012, the Swiss Federal Supreme Court upheld to a large extent the position of the Commissioner and imposed strict conditions on Google as regards the Street View services.[39]

iii Private litigation

Any person may request information from the controller of a data file as to whether personal data concerning them is being processed (Article 8 Paragraph 1 DPA). This 'right to information' includes information about the source of the personal data, the purpose of and, if applicable, the legal basis for the processing as well as the categories of the personal data processed, the other parties involved in the processing and the data recipient concerned (Article 8 Paragraph 2 DPA). Such information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge. Any data subject may also request that incorrect data be corrected (Article 5 Paragraph 2 DPA).

In addition, the data subjects have ordinary judicial remedies available under civil law to protect their personality rights (Article 15 DPA in relation to Article 28–28l of

36 According to the Swiss Federal Statistical Office, only 35 sanctions for infringements of Article 34 and Article 35 DPA have been reported during 2009 to 2014. The published statistics do not show if the sanctions relate to Article 34 or Article 35 DPA and do not mention the amount of fines that have been imposed either (see www.bfs.admin.ch/bfs/portal/de/index/themen/19/03/02/ key/01.html; last visited on 14 September 2015). Furthermore, the published statistics are incomplete and the actual number of sanctions is most likely higher.

37 Swiss Federal Supreme Court decisions dated 12 January 2015, 4A_406/2014; 4A_408/2014 (BGE 141 III 119).

38 Swiss Federal Supreme Court decision dated 17 January 2015 (BGE 139 II 7).

39 Swiss Federal Supreme Court decision dated 31 May 2012 (BGE 138 II 346).

the Swiss Civil Code). The data subjects may in particular request that data processing be stopped, that no data be disclosed to third parties, that the personal data be corrected or destroyed, compensation for moral sufferings and payment of damages or the handing over of profits. However, as regards claims for damages, it is in practice often very difficult for a data subject to prove actual damage based on privacy infringements.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The territorial scope of application of the DPA is very broad. The DPA does not only apply to the processing of personal data in Switzerland (which is the most common trigger), but – depending on the circumstances – may also apply to the processing of personal data that takes place abroad. In fact, based on an international convention or based on Article 129 Paragraph 1 and Article 130 Paragraph 3 of the Swiss Federal Act on Private International Law of 18 December 1987 (FAPIL),[40] a data subject may in some instances have the option to file an action in a Swiss court for infringement of his or her personality rights and ask the competent court to apply Swiss law even if no processing activity has taken place in Switzerland (cf. Article 139 FAPIL).[41] Based on the foregoing, foreign organisations should review compliance with the DPA even if they do not process any personal data in Switzerland or even if they do not have any presence in Switzerland, if there is a possibility that data subjects may file a claim in Switzerland and ask for the application of the DPA.

As regards foreign organisations with personal data processing operations in Switzerland (e.g., through a branch office, an affiliate or a third-party service provider), compliance with the requirements on international data transfers is another important topic if cross-border exchange of personal data is involved (e.g., in the context of centralised HR and customer relationship management systems – see Section IV, *supra*). Moreover, if a foreign organisation transfers or discloses personal data to Switzerland for the first time, additional or new obligations for the processing of such personal data may be created that did not exist beforehand.[42] We therefore strongly recommend verifying compliance with the DPA before disclosing or transferring any personal data

40 Classified compilation (SR) 291, last amended as of 1 July 2014.

41 This does, however, not apply to public law provisions of the DPA (such as the obligation to register a data file with the Commissioner or to inform the Commissioner of a transfer abroad) as such rules are governed by the principle of territoriality and only apply to facts that take place in Switzerland.

42 Such as, for example, an obligation to register a data file with the Commissioner, or there may be instances where data that before its transfer or disclosure to Switzerland was not subject to specific data protection regulations suddenly becomes subject to the data protection regulations set forth in the DPA and the DPO because of the fact that the DPA and DPO also apply to the processing of personal data pertaining to legal entities (even if, at a later stage, the data is transferred from Switzerland abroad again).

to Switzerland, before starting to process personal data in Switzerland (whether on its own or by using group companies or third-party service providers) or before cross-border exchanges of personal data in the context of a group of companies or otherwise.

IX CYBERSECURITY AND DATA BREACHES

Article 7 DPA and Articles 8–12 DPO set out the general security requirements applicable to the processing of personal data. Additionally, the Commissioner has issued a guide pertaining to technical and organisational measures to be taken when processing personal data.[43]

Neither the DPA nor the DPO currently requires data handlers to notify the Commissioner (nor any other Swiss authority) nor the data subject of any suspected or actual personal data breaches. However, depending on the circumstances, data handlers may in certain circumstances have a contractual obligation to notify data subjects of any suspected or actual personal data breaches.[44] Whether such an obligation exists in an individual case must be checked on a case-by-case basis.

In Switzerland, the cantons are generally responsible for the prosecution of misuse of information and communication technology. To fight cybercrime more efficiently, the Swiss Confederation and the Swiss cantons entered into an administrative agreement in 2001, empowering the federal authorities to assume certain responsibilities in this area. On 1 January 2014, the Swiss national coordination unit to fight internet crime, the Cybercrime Coordination Unit Switzerland (CYCO), commenced activities.[45] CYCO conducts an initial analysis of incoming reports, secures the relevant data and then forwards the matter to the competent law enforcement agencies in Switzerland and abroad.

On a Swiss federal level, the Reporting and Analysis Centre for Information Assurance (MELANI) has been established. MELANI is the product of cooperation between the Swiss Federal Finance Department and the Swiss Federal Defence Department. MELANI serves private computers and internet users (in particular providing them with information about risks relating to the use of modern information and communication technologies) as well as selected providers of critical national infrastructures (such as banks, telecommunication services providers, etc.). MELANI has created various checklists and documentation regarding IT security. In 2008, MELANI

43 'Guide for technical and organisational measures' (status as of August 2015; www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=en, last visited on 14 September 2015). Additional security requirements apply to specific sectors, such as, *inter alia*, the financial industry and the area of medical research. Such additional requirements are set forth in separate legislative acts.

44 For example, a data handler may have an obligation to inform its customers about a data breach based on an explicit contractual obligation towards its customers or based on a general contractual duty of diligence.

45 More information on CYCO is available at: https://www.cybercrime.admin.ch/kobik/en/home.html (last visited on 14 September 2015).

established GovCERT.ch, the computer emergency response team (CERT) of the Swiss government and the official national CERT of Switzerland. GovCERT.ch is a member of the Forum of Incident Response and Security Teams, and of the European Government CERTs group.

Finally, Switzerland ratified the Council of Europe Convention on Cybercrime of 2001 in 2011. The Convention entered into force for Switzerland on 1 January 2012 together with a minor amendment of the CC and the Swiss Federal Act on International Mutual Assistance in Criminal Matters of 20 March 1981.[46]

X OUTLOOK

The currently pending reform of the DPA is likely to lead to a tightening of the Swiss data protection regime. Core issues under review are a strengthening of the position of the Commissioner and of the rights of data subjects to improve the enforcement of the DPA. With the proposed revision of the DPA, the Swiss Federal Council also intends to improve data control and ownership, as well as the protection of minors. A further aim is to strengthen the rules of good practice to ensure that the data protection principles become effective at an earlier stage. However, it remains to be seen which of these possible amendments will eventually become law. As the reform is still at an early stage and will be subject to extensive discussions in the Swiss federal parliament, it is not yet foreseeable whether and to what extent the intended reforms will eventually be adopted.

46 Classified compilation (SR) 351.1, status as of 1 January 2013.

Appendix 1

ABOUT THE AUTHORS

JÜRG SCHNEIDER

Walder Wyss Ltd

Jürg Schneider is a partner with the Swiss law firm Walder Wyss Ltd. Jürg Schneider's practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. Jürg Schneider is a member of the board of directors of the International Technology Law Association and co-chair of its data protection committee. In addition, Jürg Schneider regularly publishes and lectures on ICT topics in Switzerland and abroad.

Jürg Schneider was educated at the University of Neuchâtel (lic. iur. 1992, Dr. iur. 1999). He has previously worked as a research assistant at the University of Neuchâtel, as a trainee at the legal department of the Canton of Neuchâtel and in a Neuchâtel law firm.

Jürg Schneider speaks German, French and English. He is registered with the Zurich Bar Registry and admitted to practise in all of Switzerland.

MONIQUE STURNY

Walder Wyss Ltd

Monique Sturny is an associate in the information technology, intellectual property and competition team of the Swiss law firm Walder Wyss Ltd. She advises international and domestic companies on data protection law, competition law, distribution law, contract law and information technology law matters, as well as with respect to setting up compliance programmes. She regularly represents clients in data protection and antitrust proceedings both in court and before administrative bodies. Also, she regularly publishes in her areas of practice and is co-author of a commentary on the Swiss data protection act.

Monique Sturny was educated at the University of Fribourg (lic. iur., 2002), the London School of Economics and Political Science (LLM in international business law, 2007) and the University of Berne (Dr. iur., 2013).

Monique Sturny speaks German, English and French. She is registered with the Zurich Bar Registry and is admitted to practise in all of Switzerland.

WALDER WYSS LTD
Seefeldstrasse 123
PO Box 1236
8034 Zurich
Switzerland
Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
juerg.schneider@walderwyss.com
monique.sturny@walderwyss.com
www.walderwyss.com
www.dataprotection.ch