THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 23

SWITZERLAND

Jürg Schneider, Monique Sturny and Hugh Reeves[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[2] (DPA) and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 14 June 1993[3] (DPO). Further data protection provisions governing particular issues (e.g., the processing of employee or medical data) are spread throughout a large number of legislative acts. As Switzerland is neither a member of the European Union (EU) nor of the European Economic Area (EEA), it has no general duty to implement or comply with EU laws.[4] Accordingly, Swiss data protection law has some peculiarities that differ from the legal framework provided by the EU General Data Protection Regulation[5] (GDPR). However, because of Switzerland's location in the centre of Europe and its close economic relations with the EU, 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 GDPR is also one of the aims of the ongoing reform of the DPA, which the Swiss Federal Council initiated in April 2015.

The Swiss Data Protection and Information Commissioner (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.[6] Despite the lack of drastic sanctions in respect of data protection under the current legislative regime, 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.

---

1 Jürg Schneider is a partner, Monique Sturny is a managing associate and Hugh Reeves 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 16 October 2012.

4 Specific duties exist in certain areas based on international treaties. Furthermore, the GDPR, which became effective on 25 May 2018, is not only relevant for companies located in EU and EEA Member States, but also for Swiss companies under certain circumstances, see Section II below for more detail.

5 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

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

II THE YEAR IN REVIEW

Of a number of noteworthy reforms initiated back in 2015, some are still pending and some are expected to enter into force shortly or entered into force recently.

On 1 April 2015, the Swiss Federal Council formally decided to undertake a revision of the DPA, which is still ongoing. The overarching aim of the ongoing reform of the DPA is – among others – to lay the foundations for Switzerland's ratification of the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and, where necessary in the context of the further development of the Schengen/Dublin acquis, the adaptation of the DPA to the GDPR (see Section X, for more details).

On 21 December 2016, the Federal Council issued a preliminary draft of the revised DPA. This preliminary draft was subject to a public consultation process, which ended on 4 April 2017 and, in late August 2017, the Federal Council released the results and the various opinions gathered throughout the consultation process. This in turn resulted in the establishment of a revised draft accompanied by an explanatory report of the Swiss Federal Council on 15 September 2017.[7] Subsequently to the publication of the revised draft DPA, the Swiss federal parliament decided that the revision shall be split in two phases.

In a first step, the necessary amendments shall be adopted in order to implement the Schengen/Dublin framework (EU Directive dated 27 April 2016, EC 2016/680) regarding data protection in the field of criminal prosecution as well as police and judicial cooperation.

In a second step, the remaining main revision of the DPA, which will align Swiss data protection law more closely to the substantive provisions of the GDPR and ensure compliance with the revised Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (revision of ETS No. 108, 28 January 1981) shall be discussed by the parliament. The final text will be subject to an optional referendum.

Owing to the splitting of the revision into two phases, the data protection reform will be somewhat delayed compared to the initial schedule. Entry into force of the revised DPA is now tentatively scheduled for 2019 for the first step relating to compliance with the EU Schengen/Dublin acquis and 2020 for the remaining main revision of Swiss data protection law.

The revision process of the Swiss Federal Act on the Supervision of Postal and Telecommunication Services of 18 March 2016[8] was successfully terminated, and the revised

7 The draft DPA, the explanatory report of the Swiss Federal Council and the summary of the results of the consultation process are available in German, French and Italian on the website of the Swiss Confederation at: (in German) www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-09-150.html; (in French) www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html; and (in Italian) www.ejpd.admin.ch/ejpd/it/home/aktuell/news/2017/2017-09-150.html (all sites last visited on 21 July 2018). An unofficial English translation of the draft DPA can be found at: https://www.dataprotection.ch/dpa-revision/documentation-and-english-translation/.

8 Classified compilation (SR) 780.1.

Act and the revised related ordinance[9] entered into force on 1 March 2018.[10] The main changes concern in particular the monitoring of new technologies, the tasks of the competent authority, the personal scope of application and the storage of data.[11]

The new Swiss Federal Act on Intelligence Service (the Intelligence Service Act) was approved in a referendum in September 2016 and entered into force, together with its related ordinance, on 1 September 2017.[12] The new Intelligence Service Act will bring increased monitoring competence for Swiss intelligence services and was predominantly driven by increased efforts to prevent terrorism. The expansion of surveillance options has been heavily debated and criticised for undermining privacy and other fundamental rights of data subjects.

Many Swiss companies have been conducting GDPR implementation projects recently due to the wide extraterritorial scope of application of the GDPR, and also in anticipation of the expected changes to Swiss data protection law that will bring a closer alignment of the Swiss provisions to the GDPR. The GDPR applies to the processing activities of many Swiss companies as it applies, *inter alia*, to data processing activities outside the EU and EEA that have effects in the EU or EEA (the effects doctrine). In particular, the GDPR applies to Swiss companies in connection with the targeted offering of goods or services to persons in the EU and EEA or the monitoring of behaviour of persons in the EU and EEA (Article 3 GDPR). In addition, the GDPR may become applicable if a person with habitual residence in the EU or EEA were to claim the applicability of the law of his or her state of habitual residence based on Article 139 Paragraph 1 Letter (a) of the Swiss Federal Act on Private International Law of 18 December 1987[13] (PILA) or, if the effects of an infringement of personality rights through the processing of personal data occurred in the EU or EEA, the injured person may claim the applicability of the law of the state in which the effects of the damaging act occurred and the infringing party should have foreseen that the effects would occur in that state (Article 139 Paragraph 1 Letter (b) and Paragraph 3 PILA).

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[14] guarantees the right to privacy in Article 13. The federal legislative framework for the protection of personal data mainly consists of the DPA and the DPO. Further relevant data protection provisions are contained in the Federal Ordinance on Data Protection Certification of 28 September 2007.[15] Specific data protection issues such as, *inter alia*, transfers of data abroad, and data protection in relation to employees or as regards the medical sector, are dealt with in more detail in the relevant guidelines published by the Commissioner.[16]

9 Ordinance on the Supervision of Postal and Telecommunication Services of 18 March 2016, classified compilation (SR) 780.11.

10 Classified compilation (SR) 780.1 and SR 780.11.

11 BBl 2013 2686.

12 Classified compilation (SR) 121 and SR 121.1.

13 Classified compilation [SR] 291, last amended as of 1 April 2017.

14 Classified compilation (SR) 101, last amended as of 12 February 2017.

15 Classified compilation (SR) 235.13, last amended as of 1 November 2016.

16 As mentioned in footnote 8, the guidelines are not legally binding, but do set *de facto* standards.

The DPA and DPO apply to data processing activities by private persons (i.e., individuals and legal entities) and by federal bodies. In contrast, data processing activities by cantonal and communal bodies are regulated by the cantonal data protection laws and supervised by cantonal data protection commissioners, who also issue guidance within their scope of competence. Hence, data processing activities of cantonal and communal bodies are subject to slightly different regimes in each of the 26 cantons. Unless explicitly set forth otherwise, the present chapter focuses on the Swiss federal legislation without addressing the particularities of the data protection legislation at the cantonal level.

Key definitions under the DPA[17]

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 currently 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. It is expected, however, that personal data relating to legal entities will no longer be protected under the revised DPA.

b Data subject: an individual or, currently, also a 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 permit 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. The draft of the revised DPA foresees that the term 'personality profile' shall be replaced by the term 'profiling', bringing a closer alignment to the corresponding definition provided for by the GDPR.

f Data file: any set of personal data that is searchable by data subject. It is likely that this term will no longer be used under the revised DPA.

g 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 (the draft of the revised DPA merely uses the term 'controller' instead, bringing a closer alignment to the corresponding term used in the GDPR).

As mentioned, it is likely that some terms will change under the revised data protection regime. In particular, it appears likely that 'profiling' will replace the term 'personality profiles' and the concepts of 'data file' and 'controller of the data file' will no longer be used in the

17 Article 3 DPA.

revised DPA. However, as mentioned above, the suggested amendments of the DPA are still subject to parliamentary discussions and it is thus too early to give conclusive indications as to the revised wording of the DPA.

ii General obligations for data handlers

Anyone processing personal data must observe the following general obligations.[18]

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

18 Articles 4, 5 and 7 DPA.

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 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

According to the Swiss data protection regime, the processing of personal data does not *per se* constitute a breach of the privacy rights of the data subjects concerned. Accordingly, processing in principle 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 the processing of personal data is required if the data subjects have made the data in question generally available and have not expressly restricted the data processing (Article 12 Paragraph 3 DPA). In contrast, 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 will, or if sensitive personal data or personality profiles are disclosed to third parties for such third parties' own purposes (Article 12 Paragraph 2 DPA).

In cases where a justification is required for a specific data processing, possible forms of justification are (1) consent by the data subject concerned, (2) a specific provision of Swiss (federal, cantonal and municipal) law that provides for such data processing, or (3) an overriding private or public interest[19] in the data processing in question (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 are 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;

c processes data that are neither sensitive personal data nor a personality profile to verify the creditworthiness of another person, and discloses the data to third parties for the third parties' own purposes only if the data are 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;

19 The public interest justification 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.

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; or

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

Under Swiss data protection law, processing of personal data does not require consent of the data subject concerned in all instances. As mentioned above, consent of the data subject may constitute a possible justification for a 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).[20] To the extent that the legality of data processing is based on the consent of the data subject concerned, the consent is only valid if (1) it is given voluntarily upon provision of adequate information and, (2) in case of processing of sensitive personal data or personality profiles, it is 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 the 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 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 has 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.

The draft of the revised DPA foresees that the registration duty shall be repealed and replaced with a new documentation requirement for both controllers and processors similar to the records of processing activities according to Article 30 GDPR.

20 See Article 12 Paragraph 2 Letter (c) DPA.

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.[21]

In particular, the processing of personal data may only be assigned to a cloud service provider if the 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 the 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 preserves the 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). 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

Big data offers manifold opportunities for social and scientific research and for businesses, but at the same time, it may threaten privacy rights if the processed data is not or not adequately anonymised. The DPA is not applicable to fully and completely anonymised data. In contrast, if the processing of big data involves the processing of data that has not been fully and completely anonymised (e.g., because it can be 'de-anonymised' at a later stage by merging different data files), the right to privacy and the protection of personal data need to be ensured. 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).

21 Commissioner, 'Guide to cloud computing', available at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/Internet_und_Computer/cloud-computing/guide-to-cloud-computing.html (status 2014; last visited 21 July 2018).

Cookies

Since 2007, the use of cookies has been regulated in Article 45c Letter (b) of the Telecommunications Act of 30 April 1997.[22] 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

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.[23] 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).[24]

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 the 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).[25]

Furthermore, Article 26 of Ordinance 3 to the Employment Act[26] prohibits the use of systems that monitor the behaviour of employees, except if the monitoring systems are necessary for other legitimate reasons (e.g., quality control, security requirements, technical reasons) and provided that the systems do not impair the health and mobility of the

22 Classified compilation (SR) 784.10, last amended as of 1 September 2017.

23 Ordinance of the Federal Department of the Environment, Transport, Energy and Communications on special categories of aircraft of 24 November 1994, last amended as of 19 July 2017, classified compilation (SR) 748.941.

24 Article 179 *quater* CC is also relevant in this context, which states that 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 https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/videoueberwachung/videoueberwachung-mit-drohnen-durch-private/videoueberwachung-mit-drohnen-durch-private.html (status 2014; in German; no English version available; last visited on 21 July 2018).

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

26 Ordinance 3 to the Employment Act (Healthcare) of 18 August 1993, last amended as of 1 October 2015, classified compilation (SR) 822.113.

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.[27]

Monitoring of internet and email use by employees

As regards monitoring of internet and email use by employees in particular, the following requirements apply:

a the employer shall issue a 'use policy' that describes the permitted uses the employee may make of company internet and email resources;

b constant individual analysis of log files is not allowed;

c permanent anonymous analysis of log files and random pseudonymised analysis are admissible to verify whether the use policy is complied with;

d 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

e the monitoring policy must particularly indicate the possibility of an individual analysis, the possibility of forwarding the 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.

Whistle-blowing hotlines

The use of whistle-blowing hotlines is not specifically regulated by the DPA or the CO. Hence, the general rules, in particular on data and employee protection, apply. In a nutshell and from a DPA and CO perspective, whistle-blowing hotlines can be used if certain minimum requirements are met, such as, *inter alia*:

a the transparent informing of employees, contractors, etc., about the existence of the whistle-blowing hotline;

b 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 in order to protect the ensuing investigations or the reporting person;

c adequate safeguards to protect the data subjects from false or slanderous accusations; and

d strong state-of-the-art security measures.

27 Commissioner, 'Guide on the processing of personal data in the work area' (status November 2014; https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/19--taetigkeitsbericht-2011-2012/buergeranfragen-zur-ueberwachung-am-arbeitsplatz.html, in German; no English version available; last visited on 21 July 2018).

However, 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), and in the event of transfers abroad, specific requirements must be met (see Section IV). Furthermore, and in particular in a cross-border context, whistle-blowing hotlines may be impacted by blocking statutes (see Section VI).

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:

a establish clear use regulations about what is allowed and what is prohibited;
b maintain a separation of business and private data (both technical and logical);
c ensure data security (e.g., through encryption or passwords);
d establish clear regulations on where the business data are stored;
e use of employees' own devices must be approved in advance by a person responsible within the company; and
f establish clear regulations regarding access to the device by the employer.[28]

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Any disclosure of personal data from Switzerland to countries abroad must comply with the DPA. A disclosure of data abroad occurs when personal data are transferred from Switzerland to a country outside of Switzerland or when personal data located in Switzerland are accessed from outside of Switzerland. The DPA prohibits a disclosure of personal data abroad if the transfer could seriously endanger the personality rights of the data subjects concerned. Such a danger may in particular occur if the personal data are disclosed to a country whose legislation does not guarantee an adequate protection of personal data.

The Commissioner has published a (non-binding) list of countries that provide an adequate data protection level with respect to individuals.[29] As a rule, EU and EEA countries are considered to provide an adequate data protection level relating to individuals.

With respect to data transfers to non-EU or non-EEA countries, it is necessary to check on a case-by-case basis whether the country provides an adequate level of data protection with respect to personal data pertaining to individuals and legal entities. The same applies strictly speaking for transfers of personal data relating to legal entities to EU or EEA countries.[30]

28 Commissioner, 'Bring Your Own Device (BYOD)' (available at https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/bring-your-own-device--byod-.html; in German; no English version available; last visited on 21 July 2018).

29 See list of countries at https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf (in German; no English version available; last visited on 21 July 2018).

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

If personal data are to be transferred to a country that does not provide an adequate data protection level for the personal data being transferred, the 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 are that of a contractual party;

d disclosure is essential in specific cases 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; or

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, BCR).

In case of data transfer justified under Letter (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 BCR 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,[31] 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 BCR, it is common practice to submit a copy of the rules to the Commissioner.

On 11 January 2017, the Swiss Federal Council announced the establishment of the Swiss–US Privacy Shield. This framework is separate from – but closely resembles – the EU–US Privacy Shield (which was formally adopted by the European Commission on 16 July 2016 and predates the Swiss–US Privacy Shield). It replaces the former Swiss–US Safe Harbor Framework and purports to facilitate the transfers of personal data from Switzerland to the United States. Companies based in the United States have been able to self-certify under the Swiss–US Privacy Shield since 12 April 2017.[32] For a company certified under the Swiss–US Privacy Shield an adequate level of data protection is deemed to exist for the personal data covered by the certification. Hence personal data may be transferred from Switzerland to a company based in the United States that is certified under the Swiss–US Privacy Shield even if none of the exceptions set forth in Article 6 Paragraph 2 DPA apply. As mentioned

31 See the standard contractual clauses for the transborder outsourcing of data processing accepted by the Commissioner, available at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/entreprises/anmeldung-einer-datensammlung/mustervertrag-fuer-das-outsourcing-von-datenbearbeitungen-ins-au.html (status November 2013; last visited on 21 July 2018).

32 The dedicated Privacy Shield Framework website sets up this process: www.privacyshield.gov/welcome (last visited on 21 July 2018). It also allows any interested person to consult the list of certified companies: www.privacyshield.gov/list.

above, the Swiss–US Privacy Shield is separate from the EU–US Privacy Shield. For transfers from Switzerland to the United States, the certification under the Swiss–US Privacy Shield is relevant and a certification only under the EU–US Privacy Shield is not sufficient.

V COMPANY POLICIES AND PRACTICES

According to Article 11 Paragraph 1 DPA, the private controller[33] 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 that 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 substantive and formal data protection requirements, it has become 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 the 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 those resources and possible sanctions in the event of misuse, rules on BYOD, etc.);

b a policy regarding the processing of customer personal data;

c a policy regarding the processing of supplier personal data;

d a whistle-blowing policy;

e a policy or privacy notice 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).

In contrast to other countries' legislation, the DPA does not require private data handlers to appoint a data protection officer. For this reason, and until a few years ago, companies' 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 a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files of the company in question. In fact, appointing such a 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 under the current regime

33 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).

(see Article 11a Paragraph 3 DPA in relation to Article 11a Paragraph 5 Letter (e) DPA; see also Section III.ii). Currently, over 1,000 companies have notified the Commissioner of their appointment of an independent data protection officer.

BCR 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). Despite this fact, and until recently, BCR have not been used very frequently in Switzerland.

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 of evidence for a foreign state court or for foreign regulatory proceedings constitutes an act of a foreign state. If such acts take place in Switzerland, they violate Swiss sovereignty and are prohibited by Article 271 of the Swiss Criminal Code of 21 December 1937 (CC) unless they are authorised by the appropriate Swiss authorities or are conducted by way of mutual legal assistance proceedings (a blocking statute). A violation of Article 271 CC is sanctioned with imprisonment of up to three years or a fine of up to 540,000 Swiss francs, or both. It is important to note that transferring evidence outside Switzerland for the purposes of complying with a foreign country's order requiring the production of evidence does not prevent an application of Article 271 CC. Moreover, Switzerland does not accept 'voluntary' production of evidence even if foreign procedural laws require such production. Therefore, evidence may only be handed over to foreign authorities lawfully by following mutual legal assistance proceedings or by obtaining authorisation from the competent Swiss authorities. 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 the production (Article 2 Paragraph 2 Letter (c) DPA).[34] As a consequence, and in particular, evidence containing personal data may in such cases 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.[35]

In addition to Article 271 CC, the blocking statute in 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:

a the owner of the secret relinquishes its intent to keep the information secret;
b the owner of the secret agrees to disclose this information;

34 The DPA also does 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).

35 In contrast, producing and taking evidence in purely private foreign arbitral proceedings is not subject to Article 271 CC and therefore do not require that the parties follow the requirements of mutual legal 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). 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.

c all third parties (who have a justifiable interest in keeping the information secret) consent to such a disclosure;
d Switzerland has no immediate sovereign interest in keeping the information secret; and
e 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 mutual legal assistance and disclosure takes place in accordance with the proceedings. Contrary to Article 271 CC, Article 273 CC can also be violated by activities taking place outside 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.[36] 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 the 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 the 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:
a provide information upon request of the data subject concerned under Article 8 DPA;
b provide information on the collection of sensitive personal data and personality profiles under Article 14 DPA;

36 The processing of personal data by cantonal and communal bodies is regulated by cantonal law. 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.

c 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;
d register a database with the Commissioner; or
e cooperate with the Commissioner (Article 34 DPA).

Furthermore, anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality 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).[37]

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.[38]

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.[39]

More recently, several court decisions have been rendered regarding data protection issues in connection with the granting of access to official documents based on the Swiss Federal Freedom of Information Act of 17 December 2004.[40] In three parallel rulings dated 23 August 2016,[41] the Swiss Federal Administrative Court decided on the scope of Article 19 Paragraph 4 Letter (a) and (b) DPA, according to which federal bodies shall refuse or restrict disclosure of documents, or make such disclosure subject to conditions if (1) essential public interests or clearly legitimate interests of a data subject so require; or (2) statutory duties of confidentiality or special data protection regulations so require. In the case at hand, communal bodies requested access to documents from a closed bid-rigging proceeding investigated and decided by the Swiss Competition Commission in an attempt to collect evidence for civil follow-on actions. The Swiss Federal Administrative Court held that victims of anticompetitive conduct may be granted such access to information under the conditions

37 According to the latest statistics published by the Swiss Federal Statistical Office, only 43 offences in the sense of Article 34 and Article 35 DPA have been reported during 2009 to 2015. The published statistics neither indicate whether the sanctions relate to Article 34 or Article 35 DPA nor mention the amount of fines that have been imposed. Furthermore, the published statistics may be incomplete and the actual number of sanctions may be higher.

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

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

40 Classified compilation (SR) 152.3, last amended as of 19 August 2014.

41 Swiss Federal Administrative Court decisions dated 23 August 2016, A-6334/2014, A-6320/2014 and A-6315/2014.

that the information does not contain business secrets in the sense of Article 25 of the Swiss Federal Cartel Act of 6 October 1995 (ACart)[42] and does not contain information provided by leniency applicants in the sense of Article 49a Paragraph 2 ACart.

On 11 May 2017, the Swiss Federal Administrative Court published a leading case dated 18 April 2017 relating to personality profiles and retrievability of personal data via search engines.[43] The decision, which concerns a case of the Commissioner against a Swiss economic information platform and credit agency, is final and binding as none of the parties appealed against said decision. The Swiss Federal Administrative Court came to the conclusion that personal data that in combination reveals an essential part of the personality of a data subject and that is not relevant in assessing the creditworthiness of the person in question may not be published without the consent of the data subject concerned. The Commissioner's claim that the economic information platform and credit agency's data relating to persons registered in the commercial registry should only be retrievable with search engines in the same manner as data of the official Swiss Federal Commercial Registry was rejected (search engines, in particular Google, only show search results for the Swiss Commercial Registry (i.e., www.zefix.ch) if the search name and also the term 'Zefix' are entered into the search tool). The Swiss Federal Administrative Court stated that the economic information platform and credit agency only has limited influence on the publication of search results on search engines. Also, the Swiss Federal Administrative Court pointed out that the possibility of finding data via search engines may have positive effects from a data protection perspective as it increases transparency.

Lastly, the European Court of Human Rights (ECHR), in a ruling of 18 October 2016, overruled a decision of the Swiss Federal Supreme Court in the field of publicly regulated accident insurance. The Swiss Supreme Court had previously ruled that accident insurance companies could lawfully conduct secret surveillance of the candidates for, or beneficiaries of, insurance benefits, despite the absence of a sufficiently detailed legal basis. Subsequent to the ECHR ruling, the Swiss Federal Supreme Court, on 14 July 2017, in line with the ECHR ruling, decided that, likewise, the federal social security office could not lawfully conduct secret surveillance of candidates for or beneficiaries of disability insurance. The Swiss parliament is currently drafting an amendment that provides sufficient legal basis for such surveillance by specifically setting out applicable requirements and conditions.

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:

a the source of the personal data;
b the purpose of and, if applicable, the legal basis for, the processing as well as the categories of the personal data processed;
c the other parties involved in the processing; and
d the data recipient concerned (Article 8 Paragraph 2 DPA).

42 Classified compilation (SR) 251, last amended as of 1 December 2014.

43 Swiss Federal Administrative Court decision dated 18 April 2017, A-4232/2015.

This information must normally be provided in writing, in the form of a printout or a photocopy, and is in principle free of charge (a fee of up to 300 Swiss francs may be levied in exceptional cases outlined in Article 2 DPO). Any data subject may also request that incorrect data be corrected (Article 5 Paragraph 2 DPA).

In addition, 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 the Swiss Civil Code). Data subjects may in particular request:

a that data processing be stopped;
b that no data be disclosed to third parties;
c that the personal data be corrected or destroyed;
d compensation for moral sufferings; and
e 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 not only applies 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 PILA, 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 (see Article 139 PILA).[44] 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 a cross-border exchange of personal data is involved (e.g., in the context of centralised HR and customer relationship management systems – see Section IV). Moreover, if a foreign organisation transfers or discloses personal data to Switzerland for the first time, additional or new obligations for the processing of the personal data may be created that did not exist beforehand.[45] We therefore strongly recommend verifying compliance with the DPA before disclosing or transferring any personal data to Switzerland, before starting to process personal

44 This, however, does 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.

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

data in Switzerland (whether on one's 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.[46]

Neither the DPA nor the DPO currently explicitly require data handlers to notify the Commissioner (nor any other Swiss authority) or data subjects of any suspected or actual personal data breaches (note that this is likely to change under the revised DPA).[47] However, data handlers may indeed have a duty to inform data subjects concerned based on the principles of transparency and good faith. Data handlers may in certain circumstances also have a contractual obligation to notify data subjects of any suspected or actual personal data breaches.[48] In the event that a large number of data subjects are affected, the principles of transparency and good faith may very exceptionally even result in a duty to report the incident publicly. This may in particular be the case if the data subjects concerned cannot be informed individually and there is a high probability that damages will occur if the incident is not publicly reported. Whether an obligation to notify data subjects exists (be it individually, through public reporting, or both) 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 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 its activities.[49] 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.

46 'Guide for technical and organisational measures' (status as of February 2016; https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2016/02/leitfaden_zu_dentechnischenundorganisatorischenmassnahmendesdate.pdf.download.pdf/guide_for_technicalandorganizationalmeasures.pdf, last visited on 21 July 2018). Additional security requirements apply to specific sectors such as, *inter alia*, the financial industry and the area of medical research. These additional requirements are set forth in separate legislative acts.

47 For certain specifically regulated areas, however, these duties may exist. This is the case, for instance, in the banking sector where regulatory requirements call for a notification in certain cases of data breaches (Circular 2008/21 – Operational Risks Banks, Annex 3, of the Swiss Financial Market Supervisory Authority – FINMA, available at: www.finma.ch/de/~/media/finma/dokumente/rundschreiben-archiv/finma-rs-2008-21---30-06-2017.pdf&sa=U&ved=0ahUKEwiZ8vetoovWAhUCshQKHeLuBeMQFggNMAQ&client=internal-uds-cse&usg=AFQjCNH1i9Man6e87Na3Uq4hvV8R2iGy4g, last visited on 21 July 2018).

48 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.

49 More information on CYCO is available at https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/cybercrime.html (last visited on 21 July 2018).

On a Swiss federal level, the Reporting and Analysis Centre for Information Assurance (MELANI) was established in 2004. MELANI functions as a cooperation model, *inter alia*, between the Swiss Federal Finance Department and the Swiss Federal Defence Department. It 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 and telecommunication services providers). MELANI has created various checklists and documentation regarding IT security. In 2008, MELANI established GovCERT.ch, the computer emergency response team (CERT) of the 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.[50]

X OUTLOOK

The ongoing reform of the DPA is likely to lead to a tightening of the Swiss data protection regime. Based on the publication of the draft of the revised DPA,[51] the following aspects are particularly noteworthy:

a transparency in data processing is increased. In particular, private sector actors will have a duty to inform data subjects in the event of data collection and processing;

b self-regulation shall be encouraged. Professional and business associations may prepare codes of conduct and submit them to the Commissioner for the delivery of an opinion;

c the data controller will have to perform an impact assessment whenever it appears that the envisaged data processing may lead to an increased risk to the data subjects' personality and fundamental rights, although some exceptions apply;

d a duty to notify the Commissioner or even the data subjects in cases of breach of data protection will bind data controllers;

e the present rules on personality profiles will be abolished. However, they will be replaced by new rules on profiling;

f the draft introduces the concepts of privacy by design and privacy by default. Hence, data protection must take place from the outset (i.e., from the conception of the processing) and the least invasive settings must be applied by default;

g the duty to declare data files to the Commissioner shall be abolished for private actors. Data controllers and data processors must, however, keep records of their processing activities;

h personal data relating to legal entities shall no longer be protected under the DPA;

i the Commissioner shall obtain greater powers and will in particular have the competence to render binding decisions on data controllers and processors; and

j criminal sanctions for data protection misconduct will be increased significantly. In fact, fines of up to 250,000 Swiss francs may be levied in cases of intentional offences against certain provisions of the revised DPA.

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

51 See footnote 6 for links to the draft of the revised DPA.

Moreover, the revision process will affect not only the DPA itself, but also many other laws, such as the CC, criminal procedure regulations and so forth.

The text that will eventually become law, may contain deviations from the published draft. It is nonetheless to be expected that the final revised DPA will include many of the changes suggested in the draft of the revised DPA. Entry into force of the new, revised DPA, which was initially expected to take place in 2018, should now unfold in two parts. A first part should enter into force in 2019, while the second part is tentatively expected to enter into force in 2020 (for further detail, see above Section II).

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 immediate past 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 a managing 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 the setting up of compliance programmes. She represents clients in both antitrust and data protection proceedings in court and before administrative bodies. She regularly publishes and speaks at conferences in her areas of practice.

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).

HUGH REEVES

Walder Wyss Ltd

Hugh Reeves is an associate in the information technology, intellectual property and competition team of the Swiss law firm Walder Wyss Ltd. His preferred areas of practice include technology transfers, data protection and privacy law, as well as information technology and telecommunications law. He is also active in the areas of copyright, patent, trademark and trade secret law.

Hugh Reeves was educated at the University of Lausanne (BLaw, 2008; MLaw, 2010) and the University of California at Berkeley (LLM, 2016).

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

ISBN 978-1-912228-62-1