THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-810-9

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

ACKNOWLEDGEMENTS

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

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 24

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 (DPA)[2] and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 14 June 1993 (DPO).[3] 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 (GDPR).[5] 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 reform of the DPA, which is expected to enter into force in the second half of 2022.

The Swiss Data Protection and Information Commissioner (the Commissioner) is the authority responsible 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]

---

1 Jürg Schneider and Monique Sturny are partners and Hugh Reeves is a managing associate at Walder Wyss Ltd.

2 Classified compilation (SR) 235.1, last amended on 1 March 2019.

3 Classified compilation (SR) 235.11, last amended on 16 October 2012.

4 Specific duties exist in certain areas based on international treaties. Furthermore, the General Data Protection Regulation (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 recent and noteworthy reforms, some are still pending while others have already entered into force.

On 1 April 2015, the Swiss Federal Council formally decided to revise the DPA. The overarching aim of the reform of the DPA (and the corresponding ordinances) 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 25 September 2020, the Swiss Parliament approved the final draft of the revised Data Protection Act (the revDPA).[7] In short, the revDPA comes with stricter constraints and requirements than its predecessor, the DPA. For example, the revDPA requires organisations to create and maintain an inventory of processing activities, and private controllers with a domicile or residence outside Switzerland are, under certain circumstances, required to appoint a representative in Switzerland if personal data of individuals in Switzerland is processed.

On 23 June 2021, the Swiss Federal Council published its pre-draft of the revised Swiss Federal Data Protection Ordinance (the revDPO), which will specify the provisions of the revDPA, for consultation.[8] For example, the revDPO provides for the minimum requirements for data security and the modalities of the information obligations, the data subject's access right and the notification of data security breaches. The public consultation will end on 14 October 2021. Until then, individuals or organisations wishing to participate may submit their opinion on the pre-draft to the Swiss Federal Council. After closure of the public consultation, the Swiss Federal Council will publish its consolidated draft, taking into account these submissions. The revDPO and revDPA will enter into force at the same time, which is expected to be in the second half of 2022.[9]

We encourage businesses to use the time until the revDPA's entry into force to assess its impact on their activities and start implementing or elaborating processes that will comply with the revDPA.

On 16 July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU–US Privacy Shield Framework with immediate effect while imposing additional requirements on the use of standard contractual clauses for the transfer of personal data

7 The revised DPA is available in German, French and Italian on the website of the Swiss Confederation. The German version is available at: https://www.fedlex.admin.ch/eli/fga/2017/2058/de (last visited on 26 July 2021). An unofficial English translation of the draft DPA can be found at: https://www.dataprotection.ch/user_assets/pdfs/201001-Unofficial-WalderWyss-Translation-of-the-CH-FDPA-V011.pdf (last visited on 26 July 2021).

8 The pre-draft of the revDPO is available for download in German (https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vorentw.pdf), French (https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vorentw.pdf) and Italian (https://www.bj.admin.ch/dam/bj/it/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vorentw.pdf).

9 Press release, available in German (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84103.html), French (https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-84103.html) and Italian (https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-84103.html).

to third countries.[10] Controllers and processors are now bound to verify on a case-by-case basis whether additional safeguards are necessary to ensure adequate protection of the exported personal data (e.g., due to overly broad surveillance powers of the destination country's authorities). If these additional contractual measures (e.g., a common approach in the event of requests from authorities) are not able to ensure adequate protection, the controller or processor is required to suspend or terminate the data transfer. The judgment also has implications for data transfers from Switzerland to other countries. As a reaction to the decision of the CJEU, the Commissioner stated on 8 September 2020 that, in his view, the Swiss–US Privacy Shield no longer provides an adequate data protection level for data transfers from Switzerland to recipients in the US.[11] In June 2021, the Commissioner published a guideline for assessing the legality of cross-border transfers (see Section IV).

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[12] 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.[13] Specific data protection issues such as 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.[14]

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[15]

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

10 CJEU Judgment C-311/18 of 16 July 2020.

11 The statement of the Commissioner is available at www.edoeb.admin.ch/edoeb/en/home/latest-news/media/medienmitteilungen.msg-id-80318.html (last visited on 11 September 2020).

12 Classified compilation (SR) 101, last amended on 7 March 2021.

13 Classified compilation (SR) 235.13, last amended on 1 November 2016.

14 As mentioned in footnote 6, the guidelines are not legally binding, but do set de facto standards.

15 Article 3 DPA.

entities such as corporations, associations, cooperatives or any other legal entity, as well as partnerships. The revDPA will, however, do away with the current Swiss specificity, and personal data relating to legal entities will no longer be protected.

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 revDPA 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, though an additional notion of 'high-risk profiling' introduces a discrepancy compared to the GDPR (a 'Swiss finish').

f Data file: any set of personal data that is searchable by data subject. This term will no longer be used under the revDPA.

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 revDPA merely uses the term 'controller' instead, bringing a closer alignment to the corresponding term used in the GDPR.

Moreover, as concerns data security and cybersecurity, the revDPA is more precise as it includes a definition of 'data security breaches'.[16]

ii General obligations for data handlers

Anyone processing personal data must observe the following general obligations.[17]

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.

16 Article 5, letter h of the revDPA defines a data security breach as a 'security breach which leads to an unintentional or unlawful loss, deletion, destruction or modification of personal data or to personal data being disclosed or made accessible to unauthorised person' (our translation).

17 Articles 4, 5, 7, 11, 12 and 13 DPA.

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 this recipient of personal data must disclose those uses of the personal data 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.

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 personality rights 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[18] 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;

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 automatically lead to the result 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 personality rights. The processing of personal data is only justified in situations where the interest of the data handler outweighs the interest of the data subject.

Consent

Under Swiss data protection law, processing of personal data does not, in all instances, require the data subject's consent. As mentioned above, data subject consent 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).[19] To the extent that the legality of data processing is based on the data subject's consent, the

18 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.

19 See Article 12, Paragraph 2(c) DPA.

consent, to be valid, must be given (1) voluntarily upon provision of adequate information and (2) expressly, in the case of processing of sensitive personal data or personality profiles (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 revDPA (at Article 12) foresees, instead of a registration duty, a new documentation requirement for both controllers and processors similar to the records of processing activities under Article 30 GDPR.

iii Data subject rights

Articles 8 to 10 DPA define the data subjects' access rights and their scope. Under Article 8, Paragraph 1 DPA, any person may request information from the controller of a data file as to whether data concerning them is being processed. Thereafter, the controller of a data file must notify the data subject of all available data concerning the subject in the data file, including the available information on the source of the data, and must also disclose 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 with the file and the data recipient (Article 8, Paragraph 2(a) and (b) DPA). Where processors are involved, Article 8, Paragraph 4 DPA provides that if the controller of a data file instructs a third party to process personal data, the controller remains under an obligation to provide information. The third party is under an obligation to provide information if he or she does not disclose the identity of the controller or if the controller is not domiciled in Switzerland.

Under certain circumstances, the controller of the data file may refuse or limit its disclosure. Indeed, the controller of a data file may refuse, restrict or defer the provision of information where a formal enactment so provides, or this is required to protect the overriding interests of third parties (Article 9, Paragraph 1(a) and (b) DPA), being specified that similar limitations also exist for federal bodies (Article 9, Paragraph 2 DPA). In addition, the private controller of a data file may further refuse, restrict or defer the provision of information where its own overriding interests so require, and it does not disclose the personal data to third parties (Article 9, Paragraph 4 DPA). In any case, the controller of a data file must indicate the reason for refusing, restricting or deferring access to information (Article 9, Paragraph 5 DPA), and this must take the form of a substantiated decision (Article 1, Paragraph 4 DPO).

To exercise the access right, the data subject must typically file a written request and provide proof of their identity, though an online request is also possible if the controller of the data file has made this available (Article 1, Paragraphs 1 and 2 DPO). The requested information must be provided within no more than 30 days of receipt of the request. If this

is not possible, the controller of the data file must notify the applicant accordingly with an indication of the date by which the information will be provided (Article 1, Paragraph 4 DPO). If a request for information relates to data that is being processed by a third party on behalf of the controller of the data file, the controller must pass the request on to such third party for processing if the controller is not able to provide the information itself (Article 1, Paragraph 6 DPO).

The exercise of the access right is, as a rule, free of charge for the data subject (Article 8, Paragraph 5 DPA). However, the controller of the data file may exceptionally levy from the applicant an appropriate share of the costs up to a maximum of 300 Swiss francs if the provision of information entails an unusually large amount of work, or if the applicant has already been provided with the requested information in the 12 months prior to the application and no legitimate interest in the further provision of information can be proven. A legitimate interest exists in particular if the personal data has been modified without notice being given to the data subject (Article 2 DPO).

Pursuant to Article 34 DPA, failure to provide the requested information or the provision of false or incomplete information may lead to a fine as further explained in Section VII.i.

iv Technological innovation and privacy law

In general, the electronic or online context of the data processing does not per se directly impact the applicable legal provisions, so the general provisions remain applicable. That said, certain sector-specific rules may come into play. This is the case for Article 43 of the Telecommunications Act of 30 April 1997 (TCA),[20] which imposes 'telecommunications secrecy' and provides that no person who is or has been responsible for providing a telecommunications service may disclose to a third party information relating to subscribers' communications or give anyone else an opportunity to do so. Because the definition of what constitutes a 'telecommunications service' under Swiss law is very broad and dynamic, in effect encompassing any transfer of data, be it through landlines or via new technologies such as 'over the top' delivery, telecommunications secrecy plays an important practical role also for internet service providers and web-based service providers.

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.

20 Classified compilation (SR) 784.10, last amended on 1 July 2021.

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.

The federal government has also been assessing further legal, organisational and technical measures surrounding the use of cloud services. In particular, on 1 January 2021, the Federal Council adopted its 'Cloud Strategy' in which it defines the orderly, secure and efficient use of cloud services, including from public clouds, in the federal administration.[22]

Big data

Big data offers countless opportunities for social and scientific research and for businesses. 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' (reidentification of the data subject) at a later stage by merging different data), 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).

Cookies

Since 2007, the use of cookies has been regulated in Article 45c(b) TCA. According to this provision, 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 in effect follows the opt-out principle.

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 on 26 July 2021).

22 https://www.newsd.admin.ch/newsd/message/attachments/64425.pdf.

Drones

Currently, drones of up to 30kg do not require a permit, but certain restrictions apply when flying the drones (e.g., visual contact with the drone).[23] From 1 January 2021, the revised legislation requires a specific permit for drones heavier than 25kg. Pilots and operators of drones over 250g (and also those under 250g if the drone is equipped with a camera, microphone or other sensors that are suitable for recording personal data) will have to register and take an online course and test. In general, drones must not fly over crowds of people, are required to avoid airports and nature reserves and may not fly higher than 120 metres above the ground. The 'pilot' is required to have visual contact with the drone at all times. Nowadays, drones are usually equipped with cameras – as a result, operators must be at least 12 years old. Younger 'pilots' are allowed to fly drones if supervised.[24] In addition, people using drones equipped with cameras 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 personality rights 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).[25]

v Specific regulatory areas

Processing of employee data in general

Article 328b of the Swiss Code of Obligations (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).[26]

23 Ordinance of the Federal Department of the Environment, Transport, Energy and Communications on special categories of aircraft of 24 November 1994, last amended on 1 January 2019, classified compilation (SR) 748.941.

24 'EU drone regulation in Switzerland', available at: www.bazl.admin.ch/bazl/en/home/good-to-know/drones-and-aircraft-models/Europaeische_Drohnenregulierung_uebernommen.html (last visited on 26 July 2021); 'FAQs on the new drone Regulation applicable as of 1 January 2021', available at https://www.bazl.admin.ch/dam/bazl/en/dokumente/Gut_zu_wissen/Drohnen_und_Flugmodelle/faq_neue_drohnenregulierung_2020.pdf.download.pdf/faq_neue_drohnenregulierung_2020.pdf (last visited on 26 July 2021).

25 Article 179 *quater* of the Swiss Criminal Code 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 (classified compilation (SR) 311.0); see also Commissioner, 'Video surveillance with drones by private persons', available at 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 26 July 2021).

26 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.

Furthermore, Article 26 of Ordinance 3 to the Employment Act[27] 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 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.[28]

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.

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

28 Commissioner, Guide on processing of personal data in the work area (status October 2014), https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2014/11/leitfaden_ueber_diebearbeitungvonpersonendatenimarbeitsbereich.pdf.download.pdf/leitfaden_ueber_diebearbeitungvonpersonendatenimarbeitsbereich.pdf; Commissioner, 'Guide on Internet and E-Mail Monitoring in the workplace' (available only in German, status September 2013), https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2014/06/leitfaden_internet-unde-mailueberwachungamarbeitsplatzprivatwirt.pdf.download.pdf/leitfaden_internet-unde-mailueberwachungamarbeitsplatzprivatwirt.pdf (last visited on 1 August 2021).

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:

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.

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

Using bring your own device (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.[29]

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 the legislation of which does not guarantee an adequate protection of personal data.

29 Commissioner, 'Bring Your Own Device (BYOD)' (available at www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/bring-your-own-device--byod-.html; in German; no English version available; last visited on 26 July 2021).

The Commissioner has published a (non-binding) list of countries that provide an adequate data protection level with respect to individuals.[30] 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.[31] As mentioned in Section III.i, the revDPA does away with the Swiss specificity that includes legal entities as data subjects; this change is broadly expected to simplify questions of international data transfers and bring more certainty where legal entities are concerned.

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 (e.g., the EU standard contractual clauses, where necessary supplemented and 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 (BCRs)).

In the case of data transfer justified 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 the EU standard contractual clauses adopted by the European Commission, it is sufficient to inform the Commissioner that such clauses have been entered into, and there is no need to actually submit these 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. In this context, it is noteworthy that, at the time of writing, the Commissioner has 'approved' the revised EU standard contractual clauses adopted by the European Commission in its Implementation Decision 2021/914, subject to the necessary modifications and additions in cases where

30 See list of countries at https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_d.pdf (in German; no English version available; last visited on 26 July 2021).

31 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.

the (rev)DPA applies to cross-border transfers.[32] From 27 September 2021 onwards, the Commissioner further does not recognise the standard contractual clauses adopted under the previous Data Protection Directive (Directive 95/46/EC). However, any standard contractual clauses under the Directive already concluded before said date may be continued to be used until 1 January 2023 provided the data processing subject to the standard contractual clauses remains materially unchanged. After this transitional period, existing standard contractual clauses must be replaced by those adopted as of 4 June 2021 by the European Commission. The same applies to the Swiss Transfer Data Flow Agreement of November 2013 and the Council of Europe's model contract for ensuring adequate data protection in the context of cross-border data flows previously recognised by the Commissioner.[33]

Switzerland and the United States are formally parties to the Swiss–US Privacy Shield. This framework is separate from – but closely resembles – the now-invalidated EU–US Privacy Shield (which the CJEU invalidated with immediate effect in a judgment of 16 July 2020). The Swiss–US Privacy Shield is (legally) not invalidated by the CJEU's decision. However, as a reaction to the CJEU decision, the Commissioner published a statement on 8 September 2020, according to which he deems that US corporations self-certified under the Swiss–US Privacy Shield no longer ensure an adequate level of data protection. Even though the Commissioner's assessment is only indicative (as he formally does not have the competence to invalidate the Swiss–US Privacy Shield), companies that only rely on the Swiss–US Privacy Shield should base their transfers of personal data on EU standard contractual clauses, supplemented where necessary by additional contractual safeguards and adapted to Swiss law requirements (or, although less frequently used, BCR). If EU standard contractual clauses adapted to Swiss law are already in place, their level of protection should be assessed on a case-by-case basis and, where necessary, supplemented by additional contractual safeguards. In his statement dated 8 September 2020, the Commissioner further pointed out that such contractual safeguards (even if adapted and supplemented) are not binding upon foreign authorities. Hence, the data exporter may have to implement further technical measures (such as encryption) to prevent special access to personal data by foreign authorities in the country of the data importer. If such measures are not feasible, the Commissioner recommends refraining from transferring personal data on the basis of contractual safeguards to recipients in countries that do not provide for an adequate data protection level, such as the US.

In June 2021, the Commissioner published a guideline for assessing the legality of cross-border transfers.[34] According to this guideline, it must be assessed whether (in the

32 Paper of the Commissioner on 'the transfer of personal data to a country without adequate level of data protection based on recognised standard contractual clauses and model contracts' of 27 August 2021, p. 3 (available at https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Paper%20SCC%20def.%20D%2024082021.pdf.download.pdf/Paper%20SCC%20def.%20D%2024082021.pdf in German; no English version available; last visited on 6 September 2021). The Paper provides an overview on the amendments/additions to be made.

33 Paper of the Commissioner on the transfer of personal data to a country without adequate level of data protection based on recognised standard contractual clauses and model contracts of 27 August 2021, p. 3.

34 Commissioner, Guide to checking the admissibility of direct or indirect data transfers to foreign countries (Art. 6 para. 2 letter a FADP), available at https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf, last visited on 8 September 2021.

case of access requests by local authorities in the recipient's country) (1) the powers of local authorities are sufficiently specified and based on a clear legal basis, (2) their powers and measures are proportionate, (3) the data subjects have effective legal remedies at hand according to the local law and (4) legal recourse and access to an independent and impartial court of law is guaranteed. In an annex to the guideline, the Commissioner provides an example questionnaire that may be sent to recipients of personal data in the United States for the purposes of assessing the risk of cross-border transfers.

V COMPANY POLICIES AND PRACTICES

According to Article 11, Paragraph 1 DPA, the private controller[35] 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(b) to (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);

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 key 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

35 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).

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 (see Article 11a, Paragraph 3 DPA in relation to Article 11a, Paragraph 5(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 sovereign judicial 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(c) DPA).[36] 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.[37]

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,

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

37 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 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.

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;
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.[38] 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 recommend putting an end to the data processing activity. 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 brought before 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.

38 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.

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;
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 CC).

ii Recent enforcement cases

In a judgment of 5 January 2021,[39] the Swiss Federal Supreme Court emphasised the importance of the principle of data minimisation when processing personal data. In the case before the Court, more personal data than necessary for invoicing was processed. Furthermore, the additional personal data was not collected or processed for another purpose. Although it was established that a misuse of the additionally processed personal data was impossible due to the high level of data security, the Court held – not surprisingly – that the principle of data security alone may not outweigh the principle of data minimisation. Thus, the processing of the additional personal data was held as disproportionate.

Moreover, the Swiss Federal Supreme Court dealt with two cases on access requests. In the first, it ruled that the data subject may only request access to personal data that exists physically (in contrast to personal data that can only be retrieved from memory). In particular, the access right does not comprise a right to question third parties on between whom, when and about what a personal conversation took place.[40] In the second case, the Swiss Federal Supreme Court qualified an access request as an abuse of rights because it served exclusively to clarify the prospects of a future litigation ('fishing expedition'). The Court held bad faith to be established based on the unlimited scope of the access request (pertaining to all correspondence and documents) and on the fact that the data subjects did not claim that they wished to verify the accuracy of the data or compliance with the data processing principles.[41]

A recent Swiss Federal Supreme Court case[42] dealt with the admissibility of video surveillance on company premises. According to the Swiss Federal Supreme Court, strict standards apply for video surveillance by criminal prosecution authorities. In particular, any video surveillance by police officers on company premises needs to be ordered by the Public Prosecutor and must be authorised by the competent compulsory measures court to be valid as evidence.

39 Swiss Federal Supreme Court decision of 5 January 2021, 1C_273/2020.
40 Swiss Federal Supreme Court decision of 10 December 2020, 4A_125/2020.
41 Swiss Federal Supreme Court decision of 18 November 2020, 4A_277/2020.
42 Swiss Federal Supreme Court decision of 20 December 2018, 6B_181/2018.

In a leading case dated 18 April 2017, the Swiss Federal Administrative Court dealt with the concept of 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 (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.

Moreover, 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 remains relevant. 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.[44] This case law retains its importance as the Swiss Federal Supreme Court recently dealt with additional cases arising from the above-mentioned dispute between certain Swiss banks and the United States. Indeed, the Court generally validated its prior case law and, furthermore, generally ruled that the banks that transferred their employees' personal data to the United States to comply with US governmental requests violated Swiss data protection legislation and the personality rights of the employees, though this always requires a case-by-case assessment and did not lead to valid claims for damages.[45]

Finally, the Swiss Federal Supreme Court ruled, in a 26 September 2019 judgment, that private dashcam footage does not constitute valid evidence in criminal proceedings unless it is used as evidence to solve a serious crime (which was not the case in the matter at hand).[46] In February 2021, the Swiss Federal Supreme Court confirmed its case law once more.[47] On the topic of traffic surveillance, the Swiss Federal Supreme Court moreover considered that a cantonal police act does not constitute a sufficient legal basis for automated vehicle search and identification and for traffic surveillance, as such behaviour may lead

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

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

45 Among others, Swiss Federal Supreme Court decisions of 2019, 4A_610/2018; 4A_588/2018; 4A_568/2018; 4A_50/2019; 4A_77/2019.

46 Swiss Federal Supreme Court decision of 26 September 2019, 6B_1188/2018.

47 Swiss Federal Supreme Court decision of 17 February 2021, BGer 1C_415/2020.

to a serious encroachment on constitutional rights (personal freedom and informational self-determination). Any records based on this practice, therefore, qualify as unlawfully collected evidence.[48]

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 (see Section III.iii). Any data subject may also request that incorrect data be corrected (Article 5, Paragraph 2 DPA). Under the revDPA, data subjects may further request from the controller, under certain circumstances, that their personal data is transferred to themselves or another controller (right to data portability (Article 28 revDPA)).

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 to 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 difficult for a data subject to prove actual damage based on breaches of data protection legislation and personality rights.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The territorial scope of application of the DPA is 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 of the Federal Act on Private International Law (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).[49] 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. Nonetheless, Switzerland does not have any 'data territoriality' requirements, meaning that there is no obligation to store personal data in Switzerland.

In addition, Article 3, Paragraph 1 revDPA now further clarifies that its provisions are applicable to fact patterns that have an effect in Switzerland even if they occurred abroad.

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),

48 Swiss Federal Supreme Court decision of 7 October 2019, BGE 146 I 11.

49 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.

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.[50] It is therefore strongly recommended that compliance is verified with the DPA before disclosing or transferring any personal data to Switzerland, before starting to process personal 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.

Under the revDPA, private controllers with their domicile or residence abroad are required to designate a representative in Switzerland if they process personal data of individuals in Switzerland and if such processing is connected to offering goods or services in Switzerland or to monitoring their behaviour, and if such processing is extensive, takes place regularly and involves a high risk for the personality of the data subjects.[51]

IX CYBERSECURITY AND DATA BREACHES

Article 7 DPA and Articles 8 to 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.[52]

Swiss data security requirements do not impose specific standards. Rather, and in furtherance of a technology-neutral stance, anyone processing personal data must implement technical and organisational measures that are 'adequate' (Article 8, Paragraph 2 DPO) and, in the case of automated processing, 'suitable' for achieving data security goals (Article 9, Paragraph 1 DPO). This wording is generally construed as requiring of anyone processing personal data to implement industry best practices in its cybersecurity processes.

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.[53] This will change under the revDPA, as controllers will have to report data breaches to the Commissioner if the breach could lead to a high risk to the personality or

50 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 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 is transferred abroad from Switzerland again).

51 Article 14 revDPA.

52 'A Guide for technical and organisational measures' (status as of August 2015); https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2018/TOM.pdf.download.pdf/guideTOM_en_2015.pdf, last visited on 26 July 2021). Additional security requirements apply to specific sectors such as the financial industry and the area of medical research. These additional requirements are set forth in separate legislative acts.

53 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 Authorityavailable at: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=de, last visited on 26 July 2021).

fundamental rights of the data subjects. In addition, the Swiss Federal Council is assessing the need of introducing a cyber-incident reporting obligation, which would primarily concern operators of critical infrastructures. Under the (current) DPA, however, data handlers may 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.[54] 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 particularly 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. Under the revDPA, controllers will have an explicit obligation to inform data subjects of a data security breach if this is necessary for the protection of the data subject or if the Commissioner so requests.

In Switzerland, the cantons are generally responsible for the prosecution of misuse of information and communication technology, though there are various coordination channels to enable information sharing and a fast response on the federal level as well.

On a federal level, the Ordinance on Protecting against Cyber-Risks in the Federal Administration[55] entered into force on 1 July 2020. It sets up the National Cyber Security Centre (NCSC), under the direction of the Federal Cyber Security Delegate. The NCSC merges together a kaleidoscope of agencies, including the Reporting and Analysis Centre for Information Assurance (MELANI), Federal ICT Security and the Computer Emergency Response Team (GovCERT), thereby offering a single point of contact on the federal level for all matters pertaining to cybersecurity. This latest development has been warmly welcomed and came at a time of growing awareness of cyber-risks and their potential impact on businesses and society as a whole.

X OUTLOOK

The revDPA will bring about a tightening of the Swiss data protection regime. Under the revDPA,[56] 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 will 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 breaches of data protection will bind data controllers;

54 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.

55 Classified compilation (SR) 120.73, dated 27 May 2020, entry into force on 1 July 2020, last amended on 1 April 2021.

56 See footnote 7 for links to the revDPA.

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 will 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 revDPA.

The revDPA and the revDPO are tentatively expected to enter into force in the second half of 2022 (for further details, see 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 an immediate past member of the board of directors of the International Technology Law Association and past co-chair of its data protection committee. In addition, he 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 Vaud Bar Registry and admitted to practise in all of Switzerland.

MONIQUE STURNY

Walder Wyss Ltd

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

HUGH REEVES

Walder Wyss Ltd

Hugh Reeves is a managing 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).

Hugh Reeves speaks English, French and German. He is registered with the Vaud Bar Registry and admitted to practise in all of Switzerland.

WALDER WYSS LTD

Seefeldstrasse 123
PO Box 1236
8034 Zurich
Switzerland
Tel: +41 58 658 5858
Fax: +41 58 658 5959
juerg.schneider@walderwyss.com
monique.sturny@walderwyss.com
hugh.reeves@walderwyss.com
www.walderwyss.com

an LBR business

ISBN 978-1-83862-810-9