IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

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

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 18

SWITZERLAND

Jürg Schneider, Hugh Reeves and Hannes Meyle[1]

I OVERVIEW

Swiss data protection law is set out in the revised Swiss Federal Data Protection Act of 25 September 2020 (DPA)[2] and the accompanying Swiss Federal Ordinance to the Federal Act on Data Protection of 31 August 2022 (DPO).[3] Further sector-specific data protection provisions 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. However, because of Switzerland's location in the centre of Europe and its close economic relations with the EU, Swiss law is strongly influenced by EU law.[4]

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 regularly publishes explanatory guidelines with respect to specific issues.[5]

II THE YEAR IN REVIEW

The most important recent event in terms of data protection law has been the entry into force of the fully revised DPA on 1 September 2023, together with the DPO and the Federal Ordinance on Data Protection Certification (DPCO). In short, the revision leads to stricter constraints and requirements. For example, the DPA now requires organisations to create and maintain an inventory of processing activities, and private controllers with a domicile

1 Jürg Schneider is partner, Hugh Reeves a managing associate and Hannes Meyle an associate at Walder Wyss Ltd.

2 Classified compilation (SR) 235.1, last amended on 25 September 2020.

3 Classified compilation (SR) 235.11, last amended on 31 August 2022.

4 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.

5 See https://www.edoeb.admin.ch/edoeb/de/home.html (last visited on 7 August 2023). The guidelines are not legally binding but do set de facto standards.

or residence outside Switzerland are, under certain circumstances, required to appoint a representative in Switzerland if personal data of individuals in Switzerland is processed. In addition, the sanction rules were tightened.[6]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

The Swiss Constitution of 18 April[7] 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 DPCO.

The DPA and DPO apply to data processing activities by private persons and by federal bodies, whereas cantonal and communal bodies are regulated by the cantonal data protection laws and supervised by cantonal data protection commissioners. Unless explicitly set forth otherwise, the present chapter focuses on the Swiss federal legislation.

Key definitions under the DPA

Key definitions under the DPA[8] are as follows:

a Personal data (or data): all information relating to an identified or identifiable natural person.

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

c Processing of personal data: any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data.

d Sensitive personal data: data relating to:

- religious, philosophical, 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 Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; high-risk profiling means profiling that poses a high risk to the data subject's personality or fundamental rights by matching data that allow an assessment to be made of essential aspects of the personality of a natural person;

f Controller: a private person who or federal body which, alone or jointly with others, determines the purpose and the means of processing personal data;

6 The paper of the Commissioner is available at https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/datenschutz/Paper%20SCC_DE.pdf.download.pdf/Paper%20SCC_DE.pdf (last visited on 7 August 2023).

7 Classified compilation (SR) 101, last amended on 13 February 2022.

8 Article 5 DPA.

g Processor: a private person or federal body that processes personal data on behalf of the controller;

h Breach of data security: a breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorised disclosure or access to personal data.

ii General obligations for data handlers

Anyone processing personal data must observe the following general obligations.[9]

Principle of lawfulness

Personal data must be processed lawfully, namely the processing must not violate any Swiss legislative standards, including any rules set forth in acts other than the DPA that aim at the protection of the personality rights.

Principle of good faith

Personal data must be processed in good faith; for example, 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. 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 it 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. Typically, it will be necessary to provide data subjects with a privacy notice.

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. This also applies if third parties are engaged for data processing. Detailed technical security requirements for the processing of personal data are set out in the DPO.

9 Articles 6–8 DPA.

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. Hence, processing in principle only requires a justification if it unlawfully breaches the personality rights of the data subjects, for example, 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 30, Paragraph 2 DPA).

In cases where a justification is required, possible forms of justification are: (1) consent by the data subject concerned; (2) a specific provision of Swiss law that provides for such data processing; or (3) an overriding private or public interest in the data processing in question (Article 31, Paragraph 1 DPA, with examples for overriding private interests laid out in Article 31, Paragraph 2 DPA).

Consent

Under Swiss data protection law, processing of personal data does not, in all instances, require the data subject's consent. To the extent that the legality of data processing is based on the data subject's consent, the 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 6, Paragraphs 6 and 7 DPA).

Records of processing activities

Article 12 DPA provides for a new documentation requirement, the 'records of processing activities', which is very similar to the records of processing activities under Article 30 GDPR. It applies to both controllers and processors with 250 or more employees. The controller's record shall as a minimum contain the identity of the controller, the purpose of processing, a description of the categories of data subjects and the categories of processed personal data, the categories of recipients, the retention period for the personal data or the criteria for determining this period (if possible), a general description of the measures taken to guarantee data security (if possible) and, if the data are disclosed abroad, details of the state concerned and applicable safeguards.

iii Data subject rights

Articles 25 to 29 DPA define the data subjects' access rights and their scope. Under Article 25, Paragraph 1 DPA, any person may request information from the controller as to whether and how data concerning them is being processed. Under certain circumstances, the controller may refuse or limit its disclosure, for example, where this is required to protect the overriding interests of third parties or where the request for information is obviously unjustified (Article 26, Paragraph 1 DPA). In any case, the controller must indicate the reason for refusing, restricting or deferring access to information (Article 26, Paragraph 4 DPA).

The controller must take appropriate measures to identify the data subject (Article 16, Paragraph 5 DPO), and the requested information must be provided within 30 days of receipt of the request (Article 18, Paragraph 1 DPO). If this is not possible, the controller must notify the applicant accordingly with an indication of the date by which the information will be provided (Article 18, Paragraph 2 and 3 DPO).

The exercise of the access right is principally free of charge. However, the controller may exceptionally levy from the data subject an appropriate share of the costs up to a maximum of 300 Swiss francs if providing the information involves a disproportionate cost.

Pursuant to Article 60, Paragraph 1(a) 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 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: The employer may process personal data concerning an employee in principle 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.

Furthermore, Article 26 of Ordinance 3 to the Employment Act[10] prohibits the use of systems that monitor the behaviour of employees, except if the monitoring systems are necessary for other legitimate reasons and provided that the systems do not impair the health of the employees concerned. If monitoring is required for legitimate reasons, it must remain proportionate and the employees must be informed in advance.[11]

Monitoring of internet and email use by employees

The following requirements are to be respected:

a the employer shall issue a 'use policy' to describe the permitted uses;

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 possible sanctions.

As a general rule, employers shall not read employee emails that have private content. 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.

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

11 For more information, see the guidelines published by the Commissioner, in particular: Commissioner, 'Guide on processing of personal data in the work area' (status October 2014), https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/aDSG/leitfaden_ueber_diebearbeitungvonpersonendatenimarbeitsbereich_DE.pdf.download.pdf/leitfaden_ueber_diebearbeitungvonpersonendatenimarbeitsbereich_DE.pdf.

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. 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.

Bring your own device

Bring your own device (BYOD) causes data protection concerns because of the difficulty in separating private and business data. It is recommended to respect 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.

v Technological innovation

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.

Use of cookies

The use of cookies is regulated in Article 45c(b) TCA.[12] 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 (opt-out principle).

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

Big data analytics, anonymisation

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.

Automated decision-making

The revised DPA introduces the notion of automated decision-making (i.e., a discretionary decision made exclusively based on the automated processing of personal data) when this decision has legal effects for the data subject. In this case, the data subject must be informed of the possibility to submit their opinion regarding the decision and request that it be reviewed by a human.

Data portability

Where a controller automatically processes data for the purpose of entering into or performing a contract with the data subject or on the basis of the data subject's consent, the controller must provide the personal data it receives from the data subject at any time upon request and free of charge in a commonly used electronic format.

Right to be forgotten

A right to object to data processing, which can also be referred to as the right to be forgotten, already existed under the previous DPA and remained unchanged in the revision of the law. Accordingly, the data subject may object to the processing of their personal data as a whole, or to individual aspects or characteristics.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

A disclosure of data abroad occurs when personal data are transferred from Switzerland to another country or when personal data located in Switzerland are accessed from outside 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.

The DPO (Annex 1) lists the countries that provide an adequate data protection level with respect to individuals, which lists, among others, all EU and EEA countries.

Personal data transfers to countries without an adequate level of data protection are only permitted if data privacy is guaranteed by other means (e.g., binding corporate rules, international treaties etc., see Article 16, Paragraph 2 DPA), otherwise only in very exceptional cases (e.g., overriding public interests, consent, data made publicly available by the data subject, see Article 17 DPA).

On 27 August 2021, the Commissioner 'approved' the revised EU standard contractual clauses adopted by the European Commission, subject to the necessary modifications and additions in cases where the DPA applies to cross-border transfers.[13] The standard contractual clauses adopted under the previous Data Protection Directive cannot be used anymore.

If EU standard contractual clauses adapted to Swiss law are in place, their level of protection should be assessed on a case-by-case basis[14] and, where necessary, supplemented by additional safeguards. 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.

Regarding data transfers in the US, the European Commission confirmed the adequacy of the EU–US Data Privacy Framework (the EU–US DPF) on 11 July 2023. Accordingly, from an EU perspective, no additional measures have to be taken for personal data transferred from the EU to organisations in the US that are included in the Data Privacy Framework List by the US Department of Commerce.[15] The EU–US DPF does not apply to Switzerland, but it is expected that the Swiss State Secretariat for Economic Affairs will negotiate a Swiss variant of the EU–US DPF.

V COMPANY POLICIES AND PRACTICES

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 large and medium-sized companies to effectively ensure compliance with substantive and formal data protection requirements, it has become best practice to adopt and implement various policies in this area.

Since the revision, the DPA contains provisions on the data protection officer. According to Article 10 DPA, data protection officers must exercise their function towards the controller independently and without conflicts of interest, they must have the required expertise and resources and the controller must publish the contact details of the data protection officer and notify the Commissioner thereof. In contrast to other countries' legislation, under the DPA it is not mandatory for private data handlers to appoint a data protection officer, and appointing a data protection officer has only limited benefits: where a data processing project poses a 'high risk' after a data protection impact assessment has been carried out and measures have been defined, such a project does not have to be submitted to the Commissioner if the data protection officer examines it instead (Article 23, Paragraph 4 DPA).

Nevertheless, more and more medium-sized and large companies domiciled in Switzerland have chosen to appoint a data protection officer in order to independently monitor internal compliance with data protection regulations.

13 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/datenschutz/Paper%20SCC_DE.pdf.download.pdf/Paper%20SCC_DE.pdf in German; no English version available; last visited on 7 August 2023).

14 See, e.g., the risk assessment published by the IAPP https://iapp.org/resources/article/transfer-impact-assessment-templates/ (last visited on 7 August 2023).

15 See https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en (last visited on 7 August 2023).

VI DISCOVERY AND DISCLOSURE

In Switzerland, 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) (sometimes called 'the blocking statute') unless they are authorised by the appropriate Swiss authorities or are conducted by way of mutual legal assistance proceedings. Violations may be sanctioned with imprisonment of up to three years or a fine of up to 540,000 Swiss francs, or both. 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.

By contrast, 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.[16]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Commissioner, whose powers and resources have been strengthened with the revision of the DPA, supervises compliance of both federal bodies and private persons (individuals and legal entities) with the DPA, DPO and other federal data protection regulations. The Commissioner fulfils these tasks independently.

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, in particular, order that the processing be modified, suspended or terminated, wholly or in part.

The Commissioner does not have the power to issue any fines. However, based on Article 60 et seq. DPA, the competent criminal judge may, upon complaint, sanction private individuals with a fine of up to 250,000 Swiss francs if they have wilfully:

a breached their obligations to provide information to data subjects under Articles 19, 21 and 25–27 DPA;

b disclosed personal data abroad in violation of Article 16, Paragraphs 1 and 2 DPA without satisfying the requirements of Article 17 DPA;

16 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 3 DPA).

c assigned data processing to a processor without satisfying the requirements of Article 9, Paragraphs 1 and 2 DPA;
d failed to comply with the minimum requirements for data security; or
e failed to comply with a ruling issued by the Commissioner or a decision of the appeal courts (Article 63 DPA).

Furthermore, anyone who while practising his or her profession, acquires knowledge of secret personal data for the purpose of that profession but thereafter wilfully discloses the data is, upon complaint, liable to a fine of up to 250,000 Swiss francs (Article 62 DPA).

In principle, the criminal provisions in the DPA address private individuals. Only if a fine not exceeding 50,000 Swiss francs is under consideration and the identification of the perpetrators would require disproportionate measures, the authority may decide to fine the business instead of the individuals.

ii Recent enforcement cases

The Commissioner makes available the latest statements and reports of investigations on its website. Recently, reports and recommendations have been published on the following subjects: Credit Rating and Collection Agencies, covid test centres, risk assessment for Microsoft 'M365' services, and regarding a vaccination platform.[17]

iii Private litigation

Any person may request information from the controller 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 32 DPA). 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 DPA)).

In addition, data subjects have ordinary judicial remedies available under civil law to protect their personality rights (Article 32, Paragraph 2 DPA in relation to Articles 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 DPA may also apply to the processing of personal data that takes place abroad. 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

17 For the latest reports see https://www.edoeb.admin.ch/edoeb/de/home/deredoeb/infothek/infothek-ds.html (last visited on 7 August 2023).

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).[18] Based on the foregoing, foreign organisations should review compliance with the DPA even if they do not process any personal data in Switzerland if there is a possibility that data subjects may file a claim in Switzerland. 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 DPA 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, 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).

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.[19]

IX CYBERSECURITY AND DATA BREACHES

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 1 DPA) and, in the case of automated processing, 'suitable' for achieving data security goals (Article 2 DPO, with more security requirements in Article 3 et seq. DPO).[20]

According to Article 24 DPA, controllers have to report data breaches to the Commissioner if the breach could lead to a high risk to the personality or fundamental rights of the data subjects. For specifically regulated areas, more notification duties may apply.[21] In addition, the Federal Council opened a public consultation on a revision of the new Information Security Act (ISA) – even before its full entry into force – that will provide for a

18 This, however, does not apply to public law provisions of the DPA as such rules are governed by the principle of territoriality and only apply to facts that take place in Switzerland.

19 Article 14 DPA.

20 See also the 'Guide for technical and organisational measures' by the Commissioner (status as of August 2015); https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/aDSG/guideTOM_de.pdf.download.pdf/guideTOM_de.pdf (last visited on 7 August 2023). Additional security requirements apply to specific sectors such as the financial industry and the area of medical research.

21 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 available at: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?sc_lang=de&hash=383D6884D1847665182850E88E429CCA (last visited on 7 August 2023). As of 1 January 2024, the Circular 2008/21 will be replaced by Circular 2023/1 Operational risks and resilience – banks, see https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=en&hash=1529FC7CCFD70F24BCC75C4D1B033ECF (last visited on 7 August 2023)).

general obligation of operators of critical infrastructure to report certain cyberattacks to the National Cyber Security Centre (NCSC). Furthermore, data handlers may have a duty to inform data subjects concerned if this is necessary for the protection of the data subject, based on contractual obligations or if the Commissioner so requests.

Whether an obligation to notify data subjects exists must be checked on a case-by-case basis.

On a federal level, the Ordinance on Protection against Cyber Risks in the Federal Administration[22] entered into force on 1 July 2020. It sets up the 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, Federal ICT Security and the Computer Emergency Response Team, thereby offering a single point of contact for all cybersecurity matters.

The new ISA regarding federal authorities is expected to enter into force at the beginning of 2024. Rather than setting out detailed obligations and standards itself, it is designed as an overarching law establishing a framework within which the competent federal authorities can implement adequate information security measures through ordinances and directives.

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

There are currently no specific legal requirements for secure software development or specific requirements regarding software vulnerabilities in Switzerland under the DPA.

Article 7, Paragraph 2 DPA now expressly mentions the concept of privacy by design, which forces software developers to consider privacy and data security issues from the planning stage of the development and to take appropriate measures against security threats.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

At present, there is no new legislation in Switzerland that provides for a similar regulation to the acts of the EU digital strategy (EU Digital Markets Act, Digital Services Act or Data Governance Act). However, with the updated Swiss digital strategy of January 2023,[23] the Federal Council reaffirmed its aim to continue to monitor and analyse the developments of the EU digital strategy and their impact on Switzerland and to coordinate corresponding activities and measures in Switzerland.

In a statement on a parliamentary motion of 25 August 2021,[24] the Federal Council stated that it will try to ensure that the opportunities of a European data space and the digital single market could also be used in the best possible way for Switzerland. However,

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

23 Strategie Digitale Schweiz, available at https://digital.swiss/userdata/uploads/strategie-dch-en.pdf (last visited on 7 August 2023).

24 Federal Council, Statement on the motion 'Auftrag für die Mitwirkung an der europäischen Regulierung der Digitalisierung', available at https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213676 (in German; no English version available; last visited on 7 August 2023).

the Federal Council did not see any immediate need for action. Against this background, an autonomous transposition of the acts of the EU digital strategy into Swiss law is not to be expected in the near future.

XII OUTLOOK

Under the new DPA, the Commissioner has been given more powers and also more resources. It is expected that this will lead to stricter enforcement of data protection regulations.

ISBN 978-1-80449-214-7