IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-17

DATA PROTECTION REVISITED

Report on the Law of Data Disclosure in Switzerland

Peer Sonnenberg, Timo Hoffmann

August 2022

Place of Publication

Institute for Law of the Digital Society, University of Passau

c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory

Innstraße 39, 94032 Passau

https://www.jura.uni-passau.de/irdg/

Authors

Peer Sonnenberg is a research assistant and doctoral candidate in law at the University of Passau, Chair of Public Law, Media Law and Information Law (Prof. Dr. Kai von Lewinski). His research interests include international and European data protection law with a focus on cross-border data transfer as well as European methodology. He graduated from the University of Passau with a degree in law in 2022.

Timo Hoffmann is a research assistant and doctoral candidate in law at the University of Passau, Chair of European and International Information and Data Law (Prof. Dr. Moritz Hennemann). His research interests include international and European data protection law with a focus on comparative law and anonymisation in data protection law. He graduated from the University of Passau with a degree in law in 2021.

Abstract

This report depicts the relevant law concerning individuals' disclosure of their personal data in Switzerland. Because of the expected total revision, this report does not only cover the Data Protection Act in its current version, but also the version that is to come into force by next year. This report follows a structure as to which it is possible to identify similarities and divergences between the old and the new law in various factors that might influence one's decision to disclose one's personal data, such as transparency, legal protection, or various organizational compliance. The findings shall help us establish the legal and cultural understanding of the concept of privacy in Switzerland as well as enable a comparative study with other data protection regimes worldwide.

Cite as

Sonnenberg, P. & Hoffmann, T. (2022). Data Protection Revisited - Report on the Law of Data Disclosure in Switzerland. *University of Passau IRDG Research Paper Series No. 22-17*.

Keywords

Data protection, Switzerland, Data Protection Act, data disclosure, Datenschutzgesetz, DSG, data privacy, comparative law, comparative data protection law, European law.

Contents

A. Generalities*

I. Country, People and Legends

Identification of cultural preconditions for individual data disclosure: cultural parameters that may influence decision-making concerning individual data disclosure; narratives concerning data disclosure; synonyms for "Data Protection" and "Privacy" in the local language; cultural practices and expectations concerning data disclosure and use (taboos etc.); Data protection and privacy discourse, especially call for reform.

Swiss developments on data protection have been intricately linked to developments in the European Union (EU). The Swiss **Data Protection Act** (*Datenschutzgesetz,* abbreviated DSG) was passed in 1992 and entered into force in 1993, around the same time as the Data Protection Directive[1] (abbreviated DPD), and as it is quite similar to it, mirroring Swiss *de facto* orientation towards EU regulation.[2] In 2000, Switzerland obtained the first adequacy decision under the DPD, allowing for largely unhindered data flows between EU member states and Switzerland. In the 2010s, triggered by technological developments and the drafting and subsequent enactment of the EU's General Data Protection Regulation[3] (abbreviated GDPR), **calls for reform** increased. Additionally, the EU was (and is still) set to review the adequacy decision concerning Switzerland on the basis of the stricter requirements of the GDPR and ECJ case law, a move generally seen as necessitating a reform of the DSG[4] to set higher standards of data protection. The Swiss Federal Ministry of Justice names several reasons for the revision of the DSG as follows:[5]

The law should be adapted to a **rising degree of digitalisation** of the modern world, especially regarding Big Data which awards data more and more value. Further, transparency and data subject rights shall be strengthened also in context of a digitalised world using complex algorithms and other non-transparent data processing methods. This is to be achieved by encouraging individual responsibility and introduction of concepts such as a "privacy by design" approach or documentation obligations. Last but not least, a revised DSG shall help international competitiveness especially by receiving an adequacy decision by the EU as well as to enable Switzerland to conclude a revised Schengen Association Agreement and ratify the revised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+).

After a first draft in 2017, the new DSG was passed in 2020 by the Federal Assembly. However, it has still not entered into force,

* This report is part of an interdisciplinary research project on individual data disclosure: *Vectors of Data Disclosure – A comparative study on the disclosure of personal data from the perspectives of legal, cultural studies, and business information systems research*, supported by the Bavarian Research Institute for Digital Transformation (bidt). <https://www.bidt.digital/en/vectors-data-disclosure/>. The authors would like to thank Prof. Dr. Urs Gasser for his helpful comments, Niklas Ziegler and André Rico Pacheco for their preliminary research, and Lorenz von Westerholt for his thoughtful revision of this report.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[2] Carmen Langhanke, 'Datenschutz in der Schweiz: Reichweite der europarechtlichen Vorgaben' (2014) 4(12) Zeitschrift für Datenschutz 621, 622; see on the influence of EU law and trade relations *infra* A.II.

[3] Regulation (EU) 2016/679 of the European Parliament and of 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 [2016] OJ L119/1.

[4] Because this reform will enter into force in near future, this report will cover both versions of the current and future DSG. Therefore, a distinction between the old DSG (abbreviated oDSG) and the new DSG (abbreviated nDSG) will be made.

[5] Eidgenössisches Bundesamt für Justiz, 'Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz' (21 December 2016) 17 et seq.

largely due to controversy during the drafting process of the new accompanying regulation, the Ordinance to the Federal Act on Data Protection (*Verordnung zum Datenschutzgesetz* or VDSG, the draft of which is abbreviated E-VDSG).[6] It is estimated that the VDSG, which is set to be completely revised due to said massive criticism, will be passed sometime in 2022 with both the E-VDSG and the nDSG likely entering into force on 1 September 2023[7]. According to Art. 74 para. 2 nDSG, this date depends on a decision of the Federal Council. Thus, the nDSG could still come into force later in case such a decision is not made in time.

The Swiss discourse on data protection is dominated by the **necessity of unhindered business relations** between Switzerland and EU countries[8] on one hand and scepticism of GDPR-style data protection rules based on fundamental rights on the other hand.[9] The Swiss regulation strategy can thus be described as a careful balancing act aiming at ensuring a level of data protection strict enough to retain the adequacy decision after review, while trying to keep the regulatory burden at a lower level than under the GDPR.[10] Altogether, the Swiss developments can be seen as an example of the so-called **"Brussels effect"**[11] at work, the EU commanding significant regulatory power beyond its borders.[12]

The Swiss approach to regulation tends toward business-friendly conduct while trying to comply with international rights standards: It looks to guarantee entrepreneurial freedoms that lead to cost savings on the part of the company by leaving out obligations

---

6 Main points of criticism were, that the E-VDSG – despite only being an ordinance – partially inflicted comprehensive duties on the controller, without having a sufficient legal basis in the nDSG, brings too little clarity in the concretisation of legal terms and adopts them too rigidly from the old VDSG. This can for example be seen in Art. 3 E-VDSG which – despite being located in the section titled "data security" – inflicts a duty to documentation. See Kanton Aargau, 'Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassung' (22 September 2021) 1; Kanton Bern, 'Vernehmlassung des Bundes: Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellungnahme des Kantons Bern' (15 September 2021) 1; Amédéo Wermelinger, 'Vernehmlassungsvorlage Verordnung zum Bundesgesetz über den Datenschutz' [2021] Jusletter, 5, 8.

7 Bundesamt für Justiz, 'Stärkung des Datenschutzes' (24 March 2022) <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> accessed 24 March 2022.

8 See on the relationship between the EU and Switzerland regarding business-related legislation in general Peter V Kunz, 'Europa als ein Massstab für das schweizerische Wirtschaftsrecht?: Rechtsvergleichende Fragestellungen zu einem "Weg nach Europa" anhand des neuen Kollektivanlagenrechts' in Wolfgang Wiegand and Hans P Walter (eds), *Tradition mit Weitsicht: Festschrift für Eugen Bucher zum 80. Geburtstag* (Stämpfli; Schulthess 2009).

9 David Vasella, 'Revision des DSG: Bedeutung für international tätige Unternehmen' (16 June 2021) <https://www.youtube.com/watch?v=wblMaaElIe8&t=1s> accessed 3 June 2022 who states that "Ultimately, it is a cultural difference. Traditionally, Switzerland regards data protection law, in many areas, as part of the generaly right to personality, which means it is largely the responsibility of the affected persons to look after their own right to personality. This fundamental rights approach, which is much stronger in the GDPR world, that we see it as a human right on the same level as a ban on torture, is alien to us. One could try to derive it from the Constitution, but this is not the way the courts and the authorities, and also the companies, see it." (translation ours).

10 The regulatory impact assessment in the legislative reasoning accompanying the passing of the nDSG exemplifies this perspective, see Schweizerischer Bundesrat, 'Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz' (2017) 168(45) Bundesblatt 6941, 6986 et seqq.

11 See in general Anu Bradford, *The Brussels effect: How the European Union rules the world* (Oxford University Press 2019).

12 Moritz Hennemann, 'Das Schweizer Datenschutzrecht im Wettbewerb der Rechtsordnungen' in Boris P Paal, Dörte Poelzig and Oliver Fehrenbacher (eds), *Deutsches, europäisches und vergleichendes Wirtschaftsrecht: Festschrift für Werner F. Ebke zum 70. Geburtstag* (C.H. Beck 2021).

which cause expenditure and obstacles to innovation and which – in proportion thereto – might contribute only little to privacy enhancement.[13]

It remains to be seen, therefore, how exactly the reformed Swiss data protection regulations will work in practice and whether the EU will choose to renew the adequacy decision.

II. Legal System and Lawmaking

Central characteristics; Sources of law and legal hierarchies; classification of belonging to legal spheres; Lawmakers and influential political and societal movements.

The Swiss legal system is characterized by strong elements of **direct democracy and federalism**, with many rules and laws in the hands of the 26 Swiss cantons (and about 2.400 municipalities).[14] Today's Switzerland is a federal state with regulatory responsibility and tasks interwoven between cantonal and federal level. That the Swiss system places high value on a federal division of powers promoting internal cohesion on the one hand and cultural diversity on the other hand has its reason in history: the Swiss state dates back to an alliance of independent territories in 1291 and since then attaches great importance to the pluralistic individual cantons being given comprehensive autonomy. An attempt to create a "united and indivisible republic" – the Helvetic Republic in 1798 – lasted only 5 years until it was reformed into a federal state again.[15] The modern Swiss (federal) state was created with the constitution of 1848. Over the course of the next 150 years, increasingly more legislative powers (such as criminal, economic, environmental or tax law) were passed to the Federation until the Federal Constitution of the Swiss Confederation (*Bundesverfassung der Schweizer Eidgenossenschaft*, abbreviated BV), as we know it today, reached its final revision in 1999. However, the cantons continue to enjoy a high degree of autonomy; according to Art. 3 and 42 BV, tasks that are not expressly designated federal matter are the responsibility of the cantons. Whilst the BV does not speak of explicit regulatory responsibility for data protection matters, the oDSG bases itself on Art. 95 (professional activities in the private sector), 122 (civil law) and 173 para. 2 BV (further matters that fall into the remit of the Confederation). In addition, the nDSG now names Art. 97 BV (**consumer protection**).[16] An (comprehensive) annex responsibility on the field of data processing in the relation between private parties or with federal bodies arises from this, but not when the controller is a cantonal authority.[17] This setup corresponds with the applicability of the DSG.

The Swiss constitution also knows a horizontal division of powers: The National Assembly (*Bundesversammlung*)[18] consists of the National Council (*Nationalrat*)[19] and the Council of States (*Ständerat*)[20] and forms the legislature; head of the executive branch is the Federal Council (*Bundesrat*)[21] of seven members elected by the legislature for four

[13] Jens Stark, Interview with David Rosenthal (24 November 2021) 3.

[14] Patricia Egli, *Introduction to Swiss Constitutional Law* (DIKE 2016) 40, 42.

[15] ibid 8.

[16] Interestingly enough, the oDSG did not base itself on consumer protection, showing the focus of Swiss data protection law not around fundamental rights but on privacy as a part of personality in general. That consumer protection is now named by the nDSG follows from the strengthening of transparency and responsibility of the individual which in the end benefits the consumer of data based business models, *cf.* daten:recht – das Datenrechts-Team von Walder Wyss, 'revDSG (revidierte Fassung mit Botschaft)' (23 May 2022) <https://datenrecht.ch/rev-dsg/> accessed 3 June 2022.

[17] Langhanke (n 2), 623.

[18] Art. 146 et seqq. BV.

[19] The National Council consists of 200 members elected by the people.

[20] The Council of States consists of 46 members sent by the cantons.

[21] Art. 174 et seqq. BV.

years. Head of the judiciary is the Federal Supreme Court (*Bundesgericht*)[22] in Lausanne.

If the National Assembly has the respective regulatory capacity, it may discuss and vote on legislation in both its chambers separately; a simple majority in both chambers is required to pass a new law (Art. 156 and 159 para. 2 BV). Another popular (and in this scope, unique) possibility of legislation is the Swiss **direct democracy** via (mandatory or optional) referendum, Art. 140 et seq. BV. A referendum must especially (and not exhaustively) be held if the constitution is amended or 50.000 persons eligible to vote request a referendum over a federal act within 100 days, thus giving Swiss citizens a right to veto parliamentary legislation. In this case, a vote is held which is decided by the simple majority of the votes; a quorum is not required. Such referenda occur frequently: In their long history,[23] over 600 took place, of which many were successful.[24] Another important instrument of the Swiss direct democracy system is the popular initiative (Art. 139 BV), through which Swiss citizens can demand a (partial) revision of the constitution. Since its addition to the constitution in 1891, nearly 500 popular initiatives where started, but only roughly 5 % were admitted to being voted on and thereafter also succeeded.[25]

The Swiss legal order is traditionally grouped in the **Germanic legal sphere**,[26] together with German and Austrian law, amongst others, due to its historically similar structure of (especially) private law.[27] Contrary to legal spheres where common law is predominant, the Swiss law consists of various written provisions on a constitutional and statutory level, which – alongside the interpretation of legal scholars who may have a large influence on certain developments of the law – decisively determine the individual application of law. German law has had great influence on Swiss law,[28] which can be attributed to the common language,[29] as German is the language spoken by almost two thirds of the Swiss populace. In turn, this means that French and Italian influence on legal thought can be felt as well – with much comparative law input arising from the neighbouring countries of Germany, France, Italy and Austria.[30] The **four official languages** of (federal) Switzerland (German,

---

[22] Art. 188 et seqq. BV. Literal translation "federal court".

[23] The first referendum concerned the draft of the federal constitution in 1848.

[24] Roughly 75 % of mandatory and 50 % of optional referenda, see Egli (n 14) 75.

[25] A list of all referenda and popular initiatives can be found at Universität Bern, 'swiss votes' (9 May 2022) <https://swissvotes.ch/votes?page=0> accessed 9 May 2022.

[26] Peter V Kunz, 'Instrumente der Rechtsvergleichung in der Schweiz bei der Rechtssetzung und bei der Rechtsanwendung' [2009] Zeitschrift für Vergleichende Rechtswissenschaft 31, 33. Note that comparison of laws by building the legal spheres was developed for private law and its application to public law is often rejected in principle, *c.f.* Carl-David Busse, *Die Methoden der Rechtsvergleichung im öffentlichen Recht als richterliches Instrument der Interpretation von nationalem Recht* (Nomos Verlagsgesellschaft 2015) 292 et seqq. with further proof. Under the heading of "material relativity" (*materienbezogene Relativität)*, however, a partial applicability of legal spheres in public law is recognised, *c.f.* fundamentally Konrad Zweigert and Hein Kötz, *Einführung in die Rechtsvergleichung: Auf dem Gebiete des Privatrechts* (Mohr 1996) 64.

[27] Elisabeth Berger, 'Deutscher Rechtskreis' (29 May 2022) <http://ieg-ego.eu/de/threads/crossroads/rechtsraeume-rechtskreise/elisabeth-berger-deutscher-rechtskreis> accessed 29 May 2022.

[28] Kunz, 'Instrumente der Rechtsvergleichung' (n 26) 37, noting the fact that German law is almost always considered wherever comparisons are made (there in footnote 45).

[29] See Ingeborg Schwenzer, 'Development of Comparative Law in Germany, Switzerland, and Austria' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford handbook of comparative law* (Second edition. Oxford University Press 2019) 97.

[30] See on the influence of comparative law on Swiss law generally Kunz, 'Instrumente der Rechtsvergleichung' (n 26).

Italian, French and (partially) Rhaeto-Romanic[31]) are particularly interesting in this respect, because every federal law must be passed in every language,[32] which highly influences the interpretation of wording. Nonetheless, depending on the canton some courts publish their judgements in only one language and only a summary of contents is published in German, French, Italian and English, which raises the question of nationwide uniform application of law.

In recent times, a significant influence on Swiss law can be seen in EU legislation. While Switzerland rejected EU and EEA membership in the 1990s, it has since taken the way of integration through bilateral treaties and internal action[33] - a reaction to an increasingly interdependent world and acknowledgment of the necessity of regulatory convergence towards its trade partners, as Switzerland is completely encircled by EU (and EEA, in the case of Liechtenstein) nations. Notably, the Schengen and Dublin agreements require Switzerland to dynamically implement certain acts of EU law or face termination of the agreement.[34] Further, Swiss legislation often closely follows EU rules in other parts of regulation in order to prevent differing parallel requirements for Swiss companies - this transformation is often regarded as an "**autonomous implementation**".[35] The fact that the term "Swiss Finish"[36], referring to rules explicitly divergent from EU legislation, exists as a regular term in Swiss legal discourse can be understood to show the normality of this convergent implementation of EU law.[37]

However, the obligation to conform to EU rules while not taking part in the legislative process has led to significant discontent and political controversy in Switzerland.[38] In order to recalibrate the relationship between Switzerland and the EU, beginning in 2014, steps were taken to establish the EU-Switzerland Institutional agreement.[39] In May 2021, however, talks were halted, leaving open the future of EU-Swiss relations and thus, the relationship between Swiss and EU law. Rather, Switzerland will "safeguard their well-established cooperation and (…) systematically maintain the agreements already in force".[40]

B. Information Regulation in General

I. Structure of Information Law

Constitutional and basic rights aspects; relevant regulations concerning intellectual property, secrecy, cybercrime (data privacy *aut idem infra* at C.); Which

[31] *Cf.* Art. 5 para. 1 SpG.

[32] *Cf.* Art. 10 et seq. SpG.

[33] Most prominently in this respect, Switzerland has signed the Schengen (and Dublin) Association Agreement in 2008, allowing for free passenger traffic and a simpler criminal and judicial prosecution between Switzerland and the EU.

[34] Astrid Epiney, 'Vertraglicher «Umsetzungsdruck» und «autonomer Anpassungszwang» aus Brüssel' [2014] LeGes - Gesetzgebung und Evaluation 383.

[35] ibid; Reto M Hilty, '§ 58 Schweiz' in Ulrich Loewenheim (ed), *Handbuch des Urheberrechts* (Beck-Online Bücher, 3. Auflage. C.H. Beck 2021) N 1; Thomas Jutzi, 'Der Einfluss des EU-Rechts auf das schweizerische Recht der kollektiven Kapitalanlagen' (2015) 6(1) Aktuelle Juristische Praxis 1, 5 et seq.

[36] See for examples of such "Swiss Finishes" which are in particular prominent in Swiss information obligations *infra* C.III.2.a. David Vasella and Jaqueline Sievers, 'Der "Swiss Finish" im Vorentwurf des DSG' [2017] digma - Zeitschrift für Datenrecht und Informationssicherheit 44 on a more comprehensive overview of „Swiss Finishes" in the early draft of the nDSG, some of which have been abandoned in the final version.

[37] David Rosenthal, 'Das neue Datenschutzgesetz' [2020] Jusletter, 5; Matthias Oesch, 'Die bilateralen Abkommen Schweiz-EU und die Übernahme von EU-Recht' [2017] Aktuelle Juristische Praxis (AJP) 638, 645.

[38] Oesch (n 37).

[39] ibid 639.

[40] Federal Council, 'Institutional agreement' (8 June 2022) <https://www.eda.admin.ch/europa/en/home/europapolitik/ueberblick/institutionelles-abkommen.html> accessed 8 June 2022.

regulations are based on international provisions (especially concerning intellectual property)?

Art. 13 BV contains a protection of ***Privatsphäre***, which may be translated as private sphere or privacy, and which has been interpreted broadly to contain a right to personality. It even contains an explicit right to be protected against the **misuse of one's personal data** (Art. 13 para. 2 BV), a difference when compared to other constitutions worldwide, with most drafted before prominence of the issue of data protection and privacy.

Switzerland is also party to the European Convention on Human Rights (ECHR) since 1974, which contains a right to private life in its Art. 8 and freedom of expression in its Art. 10. Compliance with these internationally acknowledged fundamental rights is therefore relevant for the interpretation and application of Swiss data protection law.

Other relevant fundamental rights in Switzerland are listed by the Data Protection and Information Commissioner (*Eidgenössicher Datenschutz- und Öffentlichkeitsbeauftragter,* abbreviated EDÖB) as important for assessing the adequacy of data protection in third countries,[41] thus allowing for the conclusion that they are - from the perspective of Swiss authorities - the backbone of its data protection law. This list contains:

- The principle of legality (Art. 5 para. 1 and Art. 164 BV). Infringement of fundamental rights (here especially privacy) must comply with a definite and clear legal basis.
- The principle of proportionality (Art. 5 para. 2 BV). The responsibilities and measures of authorities must be appropriate and necessary to fulfil its legal purposes. Also, they must be reasonable for the respective addressee of the measure.
- The right to seek effective remedies (in data protection contexts, read into Art. 13 para. 2 BV). To properly enforce rights, especially privacy and informational self-determination (*informationelle Selbstbestimmung)*[42], the individual must have access to legally consolidated remedies.
- The guarantee of access to justice and to an independent judge (Art. 29 et seqq. BV). The system of control (concerning data protection) must be effective, free of influence and impartial. This especially includes protection from arbitrariness.

II. Allocation of Informational Legal Positions

Commodity/commoditization, especially. "intellectual property"; collective goods; public goods.

Swiss intellectual property law consists of the Copyright Act (*Urheberrechtsgesetz,* abbreviated URG) and a corresponding ordinance, the Trademark Act (*Markenschutzgesetz,* abbreviated MSchG) including protection of indication of source and a corresponding ordinance, the Patents Act (*Patentgesetz,* abbreviated PatG) plus ordinance and the Designs Act *(Designgesetz*, abbreviated DesG) and yet again a corresponding ordinance.

The protection granted by the URG focuses on the definition of "works" in its Art. 2: "Works are literary and artistic intellectual creations with individual character, irrespective of their value or purpose". The primarily protected entity is the author according to Art. 6 URG being the natural person who has created the work. Even though not made explicit in the system of the URG, Swiss copyright law divides its scope of protection in two aspects: the author's moral rights to their works and their exploitation

[41] EDÖB, 'Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug (nach Art. 6 Abs. 2 lit. a) DSG)' (18 June 2021) 5; see also Nicole B Zanon and Olivia Boccali, 'Die neue Schritt-für-Schritt-Anleitung zur Übermittlung von Personendaten ins Drittland nach Schweizer Datenschutzrecht' [2022] Privacy in Germany 40, 42.

[42] See on the concept of informational self-determination as adopted by Swiss jurisprudence *infra* C.III.1.

rights.[43] Thus, the author has on one hand the right to determine the author's designation (Art. 9 para. 2 URG) or the right to decide over the integrity of his works (Art. 11 URG), on the other hand exploitation rights such as to produce copies or to perform/present a work (Art. 10 para. 2 and 3 URG). Even though disputed and the wording of Art. 16 para. 1 URG ("copyright is assignable") suggesting otherwise, the moral rights of the author cannot be transmitted in Swiss practice.[44] Further, Art. 19 et seqq. URG know some exceptions to copyright such as private use (Art. 19), temporary copies (Art. 24a) or quotation (Art. 25).

The PatG protects "new inventions applicable in industry" (Art. 1 para. 1 PatG). The invention is new if it does not form part of the state of the art, which again comprises everything made available to the public by means of a written or oral description, by use, or in any other way prior to the filing, *cf.* Art. 7 paras 1 and 2 PatG. The patent has according to Art. 8 PatG primarily the effect that its proprietor has the right to prohibit others from commercially using the protected invention.

The scope of protection of the MSchG is defined in its Art. 1: A protected trademark is a sign which is capable of distinguishing the goods or services of one undertaking from those of other undertakings, with the exception of cases listed in Art. 2 and 3 such as forms that compose the essence of the commodity, signs that are on public domain or signs that are identical to an older trademark for the same or a similar good or service. If the Swiss Federal Institute of Intellectual Property (*Eidgenössisches Institut für Geistiges Eigentum,* abbreviated IGE) accepts an application for trademark, it grants the applicant the right to exclusively use the trademark for their goods and services for the next 10 years (Art. 10 and 13 MSchG). The MSchG also grants protection for (geographical) indications of source in its Art. 47 et seqq.

Lastly, subject-matter of protection in the DesG is the design of products or parts of products that is characterised, in particular, by the arrangement of lines, surface, contours or colour, or by the materials used (Art. 1 DesG). A design is protected to the extent that it is new and has individual character (Art. 2 para. 1 DesG). This means, if a design is used by others that has the same essential features and thus produces the same overall impression as a design already registered, the holder of the registered right may prohibit using this design (Art. 8 and 9 DesG).

These IP regulations do not fundamentally deviate from other European and international provisions. This is not only due to the signing of international agreements (see at once), but also to the endeavour to make the country's own law **compatible with EU law** by means of so-called "autonomous implementation".[45]

No concept of data ownership can (nor will under the nDSG) be found in the Swiss law.[46]

III. Institutions

Information regulation authorities; private institutions (industry associations), including international institutions; government administration und cultivation of informational goods.

[43] Hilty (n 35) N 24.

[44] ibid N 85 - 86; Schweizerischer Bundesrat, 'Botschaft zu einem Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG), zu einem Bundesgesetz über den Schutz von Topographien von integrierten Schaltungen (Topographiengesetz, ToG) sowie zu einem Bundesbeschluss über verschiedene völkerrechtliche Verträge auf dem Gebiete des Urheberrechts und der verwandten Schutzrechte vom 19. Juni 1989' (1989) 140(39) Bundesblatt 477, 534.

[45] Hilty (n 35) N 1. See on autonomous implementation already *supra* A.II.

[46] Alain Schmid, Kirsten J Schmidt and Herbert Zech, 'Rechte an Daten - zum Stand der Diskussion' (2018) 21(11) sic! Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 627, 631 with further references.

The relevant national authority regarding information regulation is the EDÖB. The EDÖB and its cantonal counterpart authorities form – together with the Principality of Liechtenstein's responsible authority – a conference organization (privatim) for the promotion of federal and cantonal collaboration via exchange of information and for the effective use of shared resources.[47]

The IGE is responsible for the examination, granting and administration of intellectual property rights. It has the task to (amongst others) advise the Federal Council in IP matters, represent Switzerland on an international level as well as to manage requested property rights. The tasks are specified in Art. 2 of the Federal Act on the Statute and Tasks of the Federal Institute of Intellectual Property.

Switzerland is member of the World Intellectual Property Organization (WIPO)[48] and the European Patent Organization (EPO)[49], amongst others, and has signed its treaties and thus aligned many intellectual property provisions to international standards. Additionally, Switzerland signed the revised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+) on November 21st, 2019 but has yet to ratify it. It is, however, a member state of the Council of Europe since 1963 and therefore has ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) (which is the predecessor of the aforementioned convention) in the year of 1998. A **ratification of Convention 108+** is likely to happen alongside the coming into force of the nDSG, which holds the necessary measures to comply with the provisions of Convention 108+.[50]

Further, Switzerland is part of the Schengen area, which is important, because partial (or rather sectoral) compliance with the DPD[51] was required by Art. 2 of the Schengen Association Agreement in 2004.[52] The EU certified a sufficient level of data protection in the context of the **Schengen acquis** in its last evaluation in 2018, but already then recommended strengthening the powers of the EDÖB as well as data subjects' rights, if Switzerland wants to fulfil its duties under the agreement.[53] In order to not bear the risks of a breach of public international treaties with the European Union, the Schengen Federal Data Protection Act (*Schengen-Datenschutzgesetz*, abbreviated SDSG) was passed, entering into force in 2018, to make only the mandatory adaptions – these being in matters of criminal law[54] – to comply with

---

[47] privatim, 'Home-Seite' (24 March 2022) <https://www.privatim.ch/de/home-page/> accessed 24 March 2022.

[48] WIPO, 'Information by Country: Switzerland' (25 May 2022) <https://www.wipo.int/directory/en/details.jsp?country_code=CH> accessed 25 May 2022.

[49] EPO, 'Member states of the European Patent Organisation' (25 May 2022) <https://www.epo.org/about-us/foundation/member-states.html> accessed 25 May 2022.

[50] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 6995.

[51] Note that, naturally, the Schengen Association Agreement of 2004 cannot legally bind Switzerland to the GDPR passed in 2016.

[52] Langhanke (n 2), 623 et seq.

[53] Council Implementing Decision (7281/19) setting out a recommendation on addressing the deficiencies identified in the 2018 evaluation of Switzerland on the application of the Schengen acquis in the field of data protection.

[54] The SDSG introduced new concepts like privacy by design and default, profiling, the data protection impact assessment, or provisions concerning automated decision-making. These new concepts, however, applied only to federal bodys who processed data for purpose of criminal prosecution, discovery, or prevention of threats to public safety in context of matters of the Schengen acquis.

EU (Schengen) law requirements.[55] This early implementation was necessary, because – contrary to the GDPR – the Law Enforcement Directive[56] (abbreviated LED) passed in parallel directly affects the Schengen acquis as protected by the Schengen Association Agreement, *cf.* recital 102, 103 LED.

IV. Procedural Aspects

Control and enforcement; individual; collective; through associations; by authorities (executive and judicial).

Court organisation is left to the individual cantons to a large extent according to Art. 122 para. 2 BV.

However, the cantons are obligated under federal law to install courts of sole cantonal instance in the area of (most importantly) intellectual property rights, antitrust law and competition law, *cf.* Art. 5 para. 1 of the Swiss Civil Procedure Code (*Zivilprozessordnung,* abbreviated ZPO). This leads to a fragmentation of court organisation differing in each canton. Whilst some use one court as "cantonal supreme court", others have up to four. And whilst some rely on one organizational unit in the first instance, others have up to ten autonomous court units. However, as far as can be seen, all 26 cantons have in common that they have only two instances before a lawsuit may be passed to the jurisdiction of federal courts.[57] On the federal level, most importantly the Federal Patent Court (*Bundespatentgericht)*, the Federal Criminal Court (*Bundesstrafgericht*) and the Federal Administrative Court (*Bundesverwaltungsgericht*) exist. The last instance is the *Bundesgericht* (Federal Supreme Court): It **supervises all judgements** of all federal and cantonal courts (of last resort). Its jurisdiction, however, is limited to the violation of *inter alia* all federal laws, international law and cantonal constitutional rights, *cf.* Art. 189 BV.

Whilst controllers[58] can bring action only to the Federal Administrative Court via appeal[59] if they are addressee of an order of a federal authority (here most likely the EDÖB), the relevant judicial branch for data/privacy protection and intellectual property in general is that dealing with civil procedure.[60]

An important judicial body on the area of intellectual property is the Federal Patent Court, which has exclusive jurisdiction of (especially) validity and infringement disputes and actions for issuing a licence in respect of patents and relating interim measures (Art. 26 para. 1 of the Federal Act on the Federal Patent Court, abbreviated PatGG) and is subordinate only to the Federal Supreme Court.

C. Regulations Concerning Disclosure of Personal Data

I. Legal Structure of Data Disclosure

Existence of "Data Protection Law"; mandatory and nonmandatory regulation; Differentiation between public and private Sector; public or private sector as a role model for regulation; general or sectoral regulation; Self-regulation (codes of conduct); Basic principles of regulation [preventive ban or freedom of processing]; risk-based approach (potential for misuse;

55 Bruno Baeriswyl, 'Entwicklungen im Datenschutzrecht: Berichtszeitraum 1. Juli 2018 bis 30. Juni 2019' (2019) 115(19) SJZ 592.

56 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

57 See for a general overview Peter Bieri, 'Die Gerichte der Schweiz – eine Übersicht' [2014] Justice - Justiz - Giustizia, who himself claims no completeness in the variety of Swiss cantonal courts.

58 See on the definition of "controller" *infra* C.II.3.

59 See on the possibility of appeal *infra* C.III.4.b.

60 See on the in more detail *infra* C.III.4.b.

Protection of certain categories of data]; privileged areas [personal; family; media; research).

On a constitutional level, Art. 13 para. 2 BV states that each person has a **right to protection against misuse of its personal data**.[61]

At the core of Swiss data protection (statutory) law is the (current and future) DSG and VDSG which apply to both private actors and federal authorities as an "omnibus law"[62]. Both entities are subject to the same general regulations.[63] Nonetheless, specific provisions differ for private and public actors.[64] This division leads to the finding that regulation for data processing by public authorities is more comprehensive than for private persons.

If the controller is a cantonal authority, not the DSG but the individual cantonal data protection laws are relevant; processing by private parties, however, is always regulated by the federal DSG.[65]

All Swiss cantons have their own data protection provisions for data processing done by their authorities, with most of the cantons revising their legislation in parallel to the development on the federal level.[66]

On the federal basis, singular privacy protection regulation outside the DSG can be found on specific sectors, such as labour law (Art. 328b of the Code of Obligations (*Obligationenrecht,* abbreviated OR)) or registry law (Art. 43a ZGB).

Protection of one's privacy – detached from "data protection" – is additionally[67] granted by Swiss Civil Code (*Zivilgesetzbuch*, abbreviated ZGB) in conjunction with the definition of privacy as provided by the Swiss constitution:[68]

Art. 28 para. 1 ZGB states the elementary obligation of Swiss privacy law, which is that any person may petition the court if his **personality was unlawfully infringed**, which mirrors the provisions in the old and new DSG,[69] and frames the discussion of data protection/data privacy as an aspect of one's personality, which can be defined as the **cultural approach** to data protection in Switzerland.[70] This approach can be best seen in the reasoning for the first Swiss data protection act in 1988:[71] Its core assessment was that "the handling of personal data can be detrimental and hurtful to the data subject in various ways". Given examples for such "hurtful effects" are that a person becomes

---

[61] Translated from German: „Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten". See on the scope of this protection in more detail *infra* C.III.4.a.

[62] Sylvain Metille, 'Swiss Information Privacy and the Transborder Flow of Personal Data' (2013) 8(1) Journal of International Commercial Law and Technology 71, 75.

[63] oDSG: Art. 4 – 11a; nDSG: Art. 5 – 13.

[64] For private actors, under oDSG: Art. 12 – 15, under nDSG: Art. 30 – 32; for public actors, under oDSG Art. 16 – 25, under nDSG: Art. 33 – 42.

[65] The reason for this lies within the federal responsibility outlined *supra* A.II.

[66] Julian Powell, 'Die Revision der kantonalen Datenschutzgesetze' [2021] Jusletter, 4, 4.

[67] Or rather, the DSG grants specific privacy in addition to the general regulation in the ZGB: The FADP is intended to supplement and concretise the protection of personality; it is intended to create preconditions as to when data processing violates the personality of the data subject, *cf.* Schweizerischer Bundesrat, 'Botschaft zum Bundesgesetz über den Datenschutz (DSG)' (1988) 139(18) Bundesblatt 413, 414, 458.

[68] See on the constitutional scope of protection of privacy *infra* C.III.4.a.

[69] See on this later in this chapter.

[70] In differentiation to other data protection systems, this right as understood by Swiss authorities and legislators is not a fundamental one on a human rights basis, but a natural one, meaning that every individual must take care of his privacy to some extent on their own, *cf.* David Vasella, 'FAQ: DSGVO und neues Schweizer Datenschutzgesetz' (2021) 38:15 <https://www.youtube.com/watch?v=wblMaaElIe8&t=1s> accessed 2 June 2022.

[71] Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 416.

insecure if he does not oversee who is processing their data, or that a person receives unjust treatments due to an information with the other party that is no longer correct. The data processing itself – even for sensible data – is not regarded "hurtful" *per se*.

In order to better understand this underlying approach to privacy protection, one must bear in mind the distinction between **protection of personality as a fundamental freedom** inherently linked to the nature of an individual, and the implementation of **personality rights as subjective rights** which grant the holder the power to use and protect their personality *erga omnes*.[72]

Not only in Art. 28 ZGB, but also in Art. 12 oDSG[73], the Swiss legislator partakes in a balancing act between these two viewpoints. By linking the Swiss regulation of privacy to the concept of "violation of personality" instead of "violation of personality rights", personality as a fundamental freedom is taken into account. Privacy functions under Swiss law not in a rule-based manner in the sense that the right holder can always derive a claim from its existence, but rather in a natural one in the sense that the data subject is granted a right to be himself. If an action is taken that interferes with this right, then the data subject can legally defend himself against this infringement via Art. 28 ZGB (in conjunction with the DSG).[74]

Art. 28 para. 2 ZGB, which defines the unlawfulness of the infringement, largely mirrors the wording of the reasons for legal justification in the old and new DSG[75]. If an unlawful infringement under Art. 28 ZGB occurs, Art. 28a – 28l ZGB allow for different remedies, including a cease-and-desist order (Art. 28a para. 1 ZGB), recovery of damages (Art. 28a para. 3 ZGB in conjunction with Art. 419 et seqq. OR (agency without specific authorization)) or to enforce a right to reply (Art. 28g para. 1 ZGB).[76]

As far as the structure of the old and new DSG is concerned, they follow the same general approach: laying down generalities such as purpose, applicability, and definitions before stating general, and thereafter specific, rights and duties concerning data protection, with the latter (in case of the nDSG partially) divided into private and public sector. This section seeks to show the general structure of regulation of data protection under old and new DSG:

Art. 1 oDSG states the aim of the law: To **protect the privacy** and fundamental rights of persons when their data is processed.[77] This mirrors the context of Swiss doctrinal thought concerning data protection, which looks at data protection from the perspective of a general protection of **personality**: While the legislator could have written "protect personal data" or "protect from data processing", the data processing is taken as a given fact and the law only aims to protect personal privacy where a controller processes data.

Art. 1 nDSG has a nearly identical wording to this, except for the changing of *Daten* to *Personendaten*, which serves the editorial purpose of clarifying the scope of the DSG

---

[72] See on this in general overview Koen Lemmens, 'The Protection of Privacy between a Rights-Based and a Freedom-Based Approach: What the Swiss Example Can Teach Us' (2003) 11(3) Tilburg Foreign Law Journal 605.

[73] Art. 30 nDSG.

[74] See in more detail on this synthesis of two, at first sight, incompatible privacy doctrines Lemmens (n 72), 620 et seqq.

[75] See Art. 13 para. 1 oDSG and Art. 31 para. 1 nDSG.

[76] Translated from German, „Gegendarstellung". The right of reply gives the victim of a violation of personality in periodically published media the opportunity to compensate for the damage to reputation suffered by obliging the medium to publish a restorative text.

[77] Translated from German, "Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.".

and brings it in line with internationally common terminology in data protection legislation.

Art. 2 para. 2 oDSG speaks of the exclusions, after speaking in para. 1 of the applicability of the oDSG to processing of private and legal entities[78] done by private persons and federal bodies. Enumerated exclusions include private use (a), parliamentary discussion (b), litigation procedures (c), public registers of private law (d), and data processed by the international committee of the red cross (e).

Art. 2 paras. 2 to 4 nDSG also speak of exclusions that remain largely unchanged. However, Art. 2 para. 1 nDSG comes with one of the largest novelties of the revision already indicated by Art. 1 nDSG: Only the data of natural persons will be protected in the future.[79]

Art. 3 nDSG is a new provision not to be found in the oDSG. It deals with international applicability by stating that this law is applicable to situations that *have impact* in Switzerland, even when initiated from a foreign country. It should be noted, however, that this is merely a codification of the previous legal situation concerning international applicability[80] as established (and applied to data protection law[81]) by case law named the *Auswirkungsprinzip* or "**effects doctrine**".[82] The effects doctrine requires to the least a potential or actual interference in the privacy of a person in Switzerland that has an impact in the territory of Switzerland beyond the individual case.[83] The fact that one singular act of the processing at stake (such as the hosting of servers or the process of determining the purpose or means) is performed on Swiss territory can be sufficient under this interpretation, which is an expression of the so called territorial principle (*Territorialprinzip*).[84] A uniform definition of this principle could not be established by Swiss courts thus far. Therefore, delimitation whether the impact is sufficient or not has to be made in the individual case, which leads some voices to conclude that its scope should be adjusted to the extraterritorial applicability of the GDPR[85], thus also generating a level playing field between Switzerland and its neighbour, the EU.[86] This interpretation would also align with Art. 14 para. 1 nDSG.

The effects doctrine – detached from its concrete interpretation – follows the reasoning that as data protection aims to protect the right to personality, violations of data protection law will regularly have impact where the person whose rights are violated is or resides – thus, this *de facto* means, quite similarly to the EU's GDPR, that processing personal data of persons *in* Switzerland will have to comply with the nDSG. Therefore, a decision how far international applicability according to the effects doctrine mirrors the

---

[78] See on this topic in the context of its amendment Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7010. On the exclusion of legal entities, see *infra* C.II.2.

[79] See on the exclusion of legal entities, see *infra* C.II.2.

[80] See *e.g.* for antitrust law *Gaba* 2C_180/2014, [2016] (BGE).

[81] See for data protection law under the oDSG *Google Street View* 138 II 346, [2012] (BGE).

[82] This principle is also found in conflicts of (antitrust) laws in the jurisdiction of the EU (cf. Stephan Wernicke, 'Anmerkung zu EuGH, Urteil vom 6.9.2017 - C-413/14 P' [2017] Europäische Zeitschrift fürs Wirtschaftsrecht 850) and the US (cf. *Hartford Fire Ins. Co. v. California* 509 U.S. 764, [1993] (United States Supreme Court)), see Torsten Körber, 'Art. 1 FKVO' in Ulrich Immenga and others (eds), *Wettbewerbsrecht* (6. Auflage. C.H. Beck 2019) no. 94 et seq.

[83] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 35.

[84] ibid.

[85] Especially Art. 3 para. 2 GDPR: the so called *lex loci solutionis*.

[86] Adrian Bieri and Julian Powell, 'Die Totalrevision des Bundesgesetzes über den Datenschutz' [2020] Jusletter, N 18; Marcel Griesinger, 'Ein Überblick über das neue Schweizer Datenschutzgesetz (DSG)' [2021] Privacy in Germany 43, 47.

one of the GDPR does not necessarily need to be made in data protection contexts.

Art. 3 item e oDSG contains the definition of "bearbeiten", which can be translated as "**processing**" (a wide definition of processing is typical of data protection laws worldwide). This differs from the German term of "*ver*arbeiten" used in the GDPR. However, the different wording shall not influence the nonetheless identical prerequisites for "processing"[87], being any operation with personal data irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data.

Art. 5 item d nDSG has a substantially identical definition of "bearbeiten".

Art. 4 oDSG enumerates the **principles of data protection** which are fundamental to the Swiss approach towards data protection regulation:[88]

- Para. 1 states that personal data may only be processed lawfully (**principle of legality**).[89]
- Para. 2 indicates that processing must be carried out in good faith and must occur in a proportionate manner (**principle of good faith**).
- Para. 3 contains a concept of purpose limitation stating that personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law (**principle of purpose limitation**).
- Para. 4 states that the acquisition of personal data and the purpose of processing must be recognizable for the data subject (**principle of recognizability**[90]).
- Para. 5[91] sets forth prerequisites for consent.[92] This provision is again largely copied in Art. 6 para. 6 and 7 nDSG. However, stricter prerequisites for consent are now necessary not just for sensitive data and the old definition of a "personality profile", but for processing of sensitive data (the same), profiling with high risk by a private person[93] and any profiling by federal bodies.

Art. 5 para. 1 oDSG is also (together with Art. 7 para. 1 oDSG) a fundamental principle equal to those outlined in Art. 4 oDSG as can be seen in Art. 12 para. 2 item a oDSG. According to these principles, personal data must be kept **correct** (Art. 5) and **secure** (Art. 7).

The three articles holding the principles of the oDSG have later been largely merged into Art. 6 nDSG, which now enumerates all principles, with the exception of Art. 8 nDSG (**data security**).

The fundamental principles now outlined in Art. 6 nDSG are as follows:

Paragraphs 1 to 3 and 6 to 7 are largely equivalent to paragraphs 1 to 5 of Art. 4 oDSG. It should be noted that the purpose limitation of Art. 6 para. 3 nDSG now only requires the processing to be "compatible"[94] with its purpose. Therefore, subsequent change of purpose which is compatible with

---

[87] Griesinger (n 86), N 10.

[88] The Swiss data protection law is, altogether, a principle-based one. See on the consequential concept of "abuse legislation" for which such principles are crucially relevant later in this chapter. Therefore, Art. 4 oDSG (Art. 6 nDSG) is of central importance for the Swiss (data protection) legal system.

[89] See on the scope of this principle *infra* C.III.1.a.

[90] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 15.

[91] This paragraph is somewhat misplaced in Art. 4 oDSG concerning the principles of data protection: It might be translated as "principle of consent". However, as follows from Art. 12 para. 2 item b oDSG, the DSG relies more on the contradiction to processing and thus raises it to a *de facto* principle, which is the very opposite of consent. Art. 4 para. 5 oDSG explicitly restricts itself to cases where consent is necessary, thus relativizing the importance of consent requirements and not justifying the placement within the principles of Art. 4 oDSG.

[92] See on the prerequisites of consent *infra* C.III.1.c.

[93] See on the novelty of high-risk profiling *infra* C.II.1.

[94] Translated from German, "vereinbar".

the original purpose must no longer be recognizable for the data subject.[95]

Art. 6 para. 5 nDSG is only an ascertainment of Art. 5 para. 1 oDSG (data correctness).

The principle of recognizability in Art. 4 para. 4 oDSG was largely incorporated into the principle of purpose limitation in Art. 6 para. 3 (and para. 2[96]) nDSG.

Art. 6 para. 4 is an innovation over the oDSG. It states that personal data must be destroyed or anonymised as soon as they are no longer necessary for the purpose of processing. This can be defined as the core of a **principle of data minimisation**.[97] The oDSG knew no explicit rule for such deletion or more generally the end of the usage cycle of personal data.

Having outlined this, a core feature of Swiss data protection law is that the DSG does not follow the approach of a prohibition subject to permission. Rather, the DSG relies on the concept of prohibition of *Persönlichkeitsverletzungen* or "violations of personality": While **processing of data is generally permissible**, violations of personality as defined in the DSG[98] lead to an infringement of data protection law.

Interestingly enough, this does not apply for public authorities. In this sector the (old as well as new) DSG[99] stipulates a prohibition subject to permission: Whilst the processing of data by federal agents is generally forbidden unless an explicit law (the type of legal act is insofar irrelevant, Art. 17 para. 2 oDSG[100] *e contrario*) allows the processing. Art. 19 para. 1 oDSG[101] states several legal bases permitting disclosure. These are: the data is indispensable for the fulfilment of the statutory task of the federal body (item a); consent (item b); public disclosure without the data subject expressly prohibiting (further) disclosure (item c); wilful denial of consent to hinder legal claims or other legitimate interests (item d).

Federal bodies, however, can process data under the provisions for private actors where they act via private law (Art. 23 para. 1 oDSG[102]), which can lead to significant delimitation problems when an organization mainly fulfils public duties:[103] While, for example, the recording of contracts buying office equipment may serve the public task of ensuring availability of office equipment and thus the functioning of the administration, the appearance of the authority is nevertheless not official and therefore of a civil law nature. In this scenario, the public authority would only need to comply to the provisions concerning private entities.

As previously mentioned, the term of "**violation of personality**"[104] becomes relevant when a private actor processes

---

[95] Under old law, it would have been a privacy infringement if an online shop, who acquired data for the purpose of handling orders, later uses this data to fight against fraught. Now, this purpose would be – under consideration of individual privacy – compatible with the purpose of handling orders, *cf.* Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 15.

[96] See on this interpretation *infra* C.III.2.a.

[97] Bieri and Powell (n 86), para 4.

[98] Art. 12 oDSG or Art. 30 nDSG.

[99] Art. 17 para. 1 oDSG or Art. 34 para. 1 nDSG.

[100] Art. 34 para. 2 nDSG is insofar identical.

[101] As a novelty of the nDSG, Art. 34 para. 3 nDSG states elements of permission not only for the disclosure, but also for all data processing by federal bodys with consent (by the individual or the Federal Council) being the most prominent.

[102] Art. 40 nDSG.

[103] Lukas Bühlmann and Michael Schüepp, 'Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht' [2021] Jusletter, 7 <https://jusletter.weblaw.ch/juslissues/2021/1059.html> accessed 31 May 2022.

[104] Translated from German, „Persönlichkeitsverletzung".

personal data, Art. 12 para. 1 oDSG[105] and one assesses the lawfulness of the processing. Therefore, prohibited processing of data has two prerequisites: a violation of personality (first instance) and its unlawfulness (second instance). Whilst Art. 12 para. 2 oDSG[106] names examples of such violations (and thus implies such are always a violation of the right to one's personality), requirements for such violations are not remarkably high, so that *de facto,* many acts may be banned in principle. Art. 13 para. 1 oDSG[107] (labelled **legal justification**) defines a violation of personality as unlawful where not justified via consent, by legitimate individual or public interest, or by law.

Explicitly named in Art. 12 para. 2, a violation of personality is always given in the following cases:

- Item a: Processing of personal data contrary to the principles of Article 4, Article 5 para. 1 and Article 7 para. 1.[108]
- Item b: Processing of personal data against the data subjects' explicit will and without justification.
- Item c: Disclosure of sensitive data or of personality profiles to third parties without justification.

Only item b and c expressly require legal justification to be absent, which allowed for the interpretation that a violation of the principles of data protection cannot be justified.[109] This interpretation cannot be upheld within the nDSG, whose Art. 30 para. 2 eliminates the wording "without legal justification", thus allowing for justification of an infringement of the data processing principles. It is of important note, that the preconditions constituting a violation of personality in Art. 12 para. 2 oDSG are listed non-exhaustively. Other elements of such violation may be found in – for example – the Federal Act on Unfair Competition (*Bundesgesetz über den unlauteren Wettbewerb* (abbreviated UWG)) in the individual case.[110] This specification, however, is not necessary as such unlawful practices fall within the remit of the principle of legality in Art. 4 para. 1 and therefore Art. 12 para. 1 item a) oDSG.

Art. 12 para. 3 oDSG deals with data publicized by the data subject[111], the processing of which regularly does not violate the right to personality when processed.[112]

Art. 13 oDSG then names the legal justifications, with para. 1 stating that a violation of personality is unlawful unless it is justified by the **consent** of the data subject, by an **overriding private or public interest**, or **by law**.

Art. 13 para. 2 oDSG then lists cases where overriding interest (of *any* person)[113] is especially to be considered, which are, non-exhaustively:

- Item a: immediate connection to the conclusion or **handling of a contract**, where personal data of the contractual partner are processed.
- Item b: where there is, now or in the future, **commercial competition** and personal data is processed for this purpose without disclosing it to third parties. This provision shall underline the comprehensive Swiss economic freedom guaranteed in Art. 27 BV: As long as the threshold to industrial espionage (or other prohibition from antitrust or competition law) is not crossed,

---

[105] Art. 30 para. 1 nDSG.

[106] Art. 30 para. 2 nDSG.

[107] Art. 31 para. 1 nDSG.

[108] See above in this chapter. This provision constitutes the core of the Swiss principle-based data protection regulation.

[109] This interpretation is disputed even for the oDSG. The prevailing literature applies elements of justification in a very restrictive way, cf. Amedeo Wemelinger, 'Art. 12' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 167 with further proof.; See also 136 II 508, [2010] (BGE) E.5.2.4.

[110] Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 459.

[111] Hereafter referred to as "publicised data".

[112] See on publicised data *infra* C.II.3.

[113] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 18.

businesses should have the freedom to internally analyse data to strengthen their own market position and learn from their competitors.[114]

- Item c: verification of creditworthiness (excluding sensitive personal data or personality profiles)[115] and – in case of data being disclosed to third parties – where needed for the conclusion or the performance of a contract with the data subject.
- Item d: processing on a professional basis exclusively for publication in the edited section of a periodically published medium (**media privilege**).
- Item e: non-personal-related uses in research, planning and statistics without identifiability of the affected persons.
- Item f: data relating to a **person of public interest** and their public activities.

The underlying concept as outlined above remains largely unchanged in the nDSG: In Art. 30 para. 1, the central obligation for processing by private persons is identical to Art. 12 para. 1 oDSG, prohibiting the unlawful violation of personality of data subjects.[116] Art. 30 nDSG specifies, non-exhaustively, situations which can constitute such violations of personality, while Art. 31 states in para. 1 that a violation of personality is in general not considered unlawful when justified by consent, overriding private or public interest or by law The paragraphs thereafter enumerate (still non-exhaustively) situations where such overriding interest are to be considered (which are the same as under the old law).[117] In comparison to the oDSG, the examples for prevailing interest are much more detailed, which allows for the interpretation that prevailing interest as legal justification should have a **narrow scope of application**.[118]

In this approach to unlawful data processing lies the central characteristic of the Swiss data protection law: It aims to regulate data protection by implementing an **"abuse legislation"** and focuses on the guarantee of fundamental principles instead of generally prohibiting processing.[119] This constitutes an underlying **principle-based data protection regulation** in divergence to a rule-based regulation which can be found within – for example – the GDPR. Justification under the Swiss regulation must not always be given, but only if the data is used differently than intended or other fundamental principles of Swiss data protection law are breached (*i.e.* "abused").[120] By setting abusive behaviour as a precondition, a data protection infringement is less likely to be triggered than it would have been under the opposite approach of a general prohibition of processing (with subject to permission) or – in other words – a strictly rule-based data protection regulation.

Overall, the Swiss approach does not focus on the concept of consent. Rather, it relies on an **opt-out regulation** in Art. 12 para. 2 item b oDSG. Consent is therefore only necessary on the secondary instance of assessing prohibited data processing when it comes to legal justification and can be substituted by particular overriding interests, which is comprehensively exemplified in Art. 13 para.

---

[114] Amédéo Wermelinger, 'Art. 13' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 181 et seq.

[115] See on the definition on these categories of data *infra* C.II.1.

[116] It must be noted in this respect, that the data subject whose privacy is violated can now no longer be a legal entity, *cf. infra* C.II.2.

[117] Note that the law does not state that conduct falling under one of the variants in items a to f is always justified. Therefore, violations of personality can still be unjustified under exceptional circumstances despite being listed here.

[118] Even though this change in interpretation must first be acknowledged by legal practice when the nDSG comes into force, it nonetheless allows for a more precise (in comparison to Art. 13 para. 2 oDSG) definition of prevailing interest.

[119] Jens Stark, Interview with David Rosenthal (24 November 2021).

[120] ibid.

2 oDSG, thus giving clarity for the controller. Nonetheless, consent gives the controller more certainty than only relying on overriding interest, which is inherently vague. These **system nudges** (or rather its preconditions) remain the same under the nDSG, with the only difference that now, the more precise definition of overriding interest in Art. 31 para. 2 allows for **more legal certainty** and might provide more confidence when basing the justification on one's data processing only on an overriding interest.

II. Concepts and Terms for Such Data

1. Personal Data as a Matter of Protection

Situational (spoken words etc.); local (at home); logical ("spheres"); informational (datum, information); Treatment of public or publicized data; limitations and expansions of definition; categories.

Art. 3 oDSG contains all the relevant definitions of the oDSG: Item a defines **personal data** as all information relating to an identified or identifiable person, whereas "information" is understood broadly and can be a conclusion of facts as well as a value judgement (for example expression of opinion)[121] and "person" can mean a legal or natural entity, according to Art. 2 para. 1 oDSG. This is *almost* the same under the nDSG with the only difference that the word "natural" person is added which omits a peculiarity of Swiss data protection regulation: its protection of personal data of legal entities.[122]

Art. 3 item c oDSG holds the concept of **"sensitive data"** as it is common in data protection laws worldwide and contains data on religious and similar views and activities (1), health, the intimate sphere and racial origin (2), social security measures (3), and administrative or criminal proceedings and sanctions (4). Art. 5 item c nDSG retains the concept of sensitive data by large, but in an effort to comply with Convention 108+[123] includes two additional categories of data considered sensitive, these being "genetic data" (3) and "biometric data uniquely identifying a natural person" (4).

Art. 3 item d oDSG contains the definition of a **personality profile**: a collection of data that permits an assessment of essential characteristics of the personality of a natural person. This definition is somewhat blurry and requires assessment in the individual case under consideration of all circumstances. The relevant factor is the risk for the individuals fundamental and personality rights which emanate from such data collections that enable an evaluation of even partial characteristics of one's own personality (this constitutes a **risk-based** approach).[124] In view of today's technical possibilities, even in itself non-sensitive data can be – if gathered to a large extent or deconstructed with advanced analysis tools – part of a personality profile.[125] Certain stricter rules under the oDSG (for example, information obligation, Art. 14 oDSG or express consent, Art. 4 para. 5) are applied to the creation of personality profiles. This concept was abolished in the nDSG and exchanged with the new concepts of profiling and high-risk profiling:

Profiling is defined in Art. 5 item f nDSG as any automated processing of personal data involving the use of such data for the purpose of evaluating certain personal aspects relating to a natural person. The relevant personality aspects (of which the analysis or prediction is

---

[121] Beat Rudin, 'Art. 3' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 13.

[122] See on protection of legal entities *infra* C.II.2.

[123] *i.e.* Art. 6 para. 1 of Convention 108+, see Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7020.

[124] Rudin (n 121) 40 et seq. with further proof.

[125] *Google* (n 81) E.8.2.

possible) are non-exhaustively exemplified as, for example, work performance, economic situation, health, personal preferences, and interests. Even though the risk-based concept of characteristics of personality remains the same, "profiling" in differentiation to "personality profiles" now does not define a static result of data processing, but rather includes the processing of characteristics itself. Thereby, the term is adjusted to European regulation and now addresses the automatic evaluation of personal data followed by an automated assessment of this data.[126] If the profiling leads to a high risk for one's personality or fundamental rights, because it combines data that indicate essential characteristics of the data subject, the nDSG now knows special regulation for this new concept of **high-risk profiling** defined in Art. 5 item g nDSG. While the term "profiling" is broader than "personality profiles"[127], "high-risk profiling" is somewhat narrower: Art. 5 item g nDSG requires – in addition to automated processing – an actual, not only potential risk; the automated processing of essential characteristics *per se* does not constitute such high risk.[128] Apart from this, high-risk profiling assimilates the concept of personality profiles.

In the private economic relationships of individuals with one another, these changes do not have a major impact: The most notable is that in Art. 6 para. 7 nDSG, express consent is only necessary for high-risk profiling (instead of for personality profiles as before). This can be seen as relaxation to some extent, depending on how narrow or broad the concept of high-risk profiling will be understood in practice in comparison to that of personality profiles.

Art. 3 item g oDSG defines a **data file** as any set of personal data that is structured in a manner such that the data is accessible by the data subject. It must be a data set that relates to a plurality of persons and is identifiable according to the persons concerned.[129] The term "data file" originates from a time where data was compiled in analogue systems such as index cards or files. Today, a data file must be understood, according to technical developments, as any electronic filing system which can be searched.[130] Data files (or rather their controller, Art. 3 item i oDSG) are therefore a very common (and central) concept of the oDSG. This concept of a data file is relevant for various rules of the oDSG such as the right to information[131] or the public register[132] but was abolished under the nDSG and has been replaced by the introduction of the even broader concept of the "controller"[133].

Art. 5 nDSG adds the definitions of **controller**[134] and **processor**[135]**,** both of which have been unknown to the earlier data protection regulation.[136] It also defines a "**breach of data security**" (item h) as "a breach of security that leads to an involuntary or unlawful disclosure or loss", *inter alia,* of personal data, which is relevant for breach

---

126 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7021 et seq.

127 Profiling is relevant for not only essential, but all characteristics plus it now includes the processing itself and not only the result of the same. Nonetheless, profiling does only apply for automated processing, which, however, can be assumed often in todays digitalized world.

128 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 11.

129 Rudin (n 121) 44.

130 ibid.

131 See on the right to information *infra* C.III.3.a.

132 See on the register of data files *infra* C.IV.1.c.

133 See on this definition *infra* C.II.3.

134 Translated from German, "Verantwortlicher", which follows the terminology of the GDPR.

135 Translated from German, "Auftragsbearbeiter", which also follows the terminology of the GDPR and deviates from the wording "bearbeiten" in Art. 5 item d nDSG, which has no semantic difference to the GDPR's "verarbeiten".

136 See on the person of the data receiver *infra* C.II.3.

notifications under Art. 24 nDSG[137] and a violation of the principle of data security in Art. 8 nDSG and thus the question whether there is a violation of personality under Art. 30 para. 2 item a nDSG. A breach of security will become relevant if one is to assess the legality of concrete data processing. To keep data secure is therefore not a completely "objective" obligation.

Central aspects of "security" in this context are the guarantees of confidentiality, integrity and accessibility of personal data, which shall not be affected in an unforeseen manner.[138] Thereby, a breach of data security must be delimited from "simple" privacy infringements, where data is misused in terms of *e.g.* disproportionate use or use for wrongful purposes.

2. Attribution of Data to Individual Persons

Creation; possession/control; personal connection; differentiation between domestic and foreign nationals; treatment of multi-referential data; limitations and expansions of definition; categories.

Art. 3 item b oDSG – contrary to Art. 1 and Art. 5 item b nDSG – speaks of natural *and* **legal entities**, thus implying that all legal entities such as private businesses or public institutions are worthy of protection when it comes to data concerning them as entity.[139] This unique concept goes back to a decision of the Swiss Federal Court in 1905,[140] which stated that legal entities shall have – to a certain extent – a **"commercial honour"**. In the following years, case law broadened the scope of this "commercial honour" and developed – amongst others – the protection of the commercial reputation of a business protected by Art. 28 ZGB.[141] That this concept was later adopted in data protection law was reasoned as follows:[142]

It would interfere with standing case law to not grant legal entities data protection whilst Art. 57 (and Art. 28) ZGB grants them privacy. Also, legal and natural entities have, in this respect, similar needs for protection; for example, data related to a small business is easily traced back to the natural person standing behind this business. Even if granted a gradual system of protection, this would lead to an – of the perspective of the Federal Council – illegitimate favourable treatment of natural persons participating in economic life. However, the argument that the legal protection of legal entities is deeply rooted in Swiss legal tradition can be identified as decisive.[143]

To consequently avoid an incomplete level of protection, "legal entity" must be understood broadly and includes legal communities without legal personality.[144]

This unique feature was abandoned with the reform of the DSG, see Art. 1 and 5 item b nDSG. The Federal Council now sees only little practical relevance of this concept and wants to adjust the Swiss concept to the rest of the world. The protection that legal entities gain from especially Art. 28 – 29 ZGB and the UWG is considered sufficient to secure the constitutional right of privacy as granted also to legal entities by Art. 13 BV.[145] With this decision, the legislator also reacted to criticism from legal scholars against data

---

137 See on notification duties *infra* C.IV.1.b.

138 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 59.

139 Damian George, 'Juristische Personen als Subjekte der Datenschutzgesetzgebung' [2016] Jusletter.

140 31 II 242, [1905] (BGE).

141 90 II 351, [1926] (BGE); this was later extended to all rights under Art 27 et seqq. ZGB unless they prerequisite human characteristics, cf. 95 II 481, [1969] (BGE), E. 4.

142 See overall: Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 439.

143 George (n 139), 9 et seq.

144 ibid.

145 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7011. Also note, that the Swiss data protection law does not focus on a fundamental rights approach but rather on a natural understanding of personality. The threshold for sufficiency of protection of constitutional rights can be regarded as rather low.

protection for legal entities. Further arguments for this change were that it legally enables unhindered data transfer to other countries (which do not know data protection for legal entities), that transparency of businesses is increased and that Art. 57 ZGB awards privacy rights only in individual cases. Supporter of this change conclude from the latter that it is no breach of tradition – as voiced by dissenting opinions[146] – to not grant legal entities a comprehensive right to data protection.[147]

To avoid the contradiction that legal entities still enjoy privacy on a constitutional level (Art. 13 and 27 BV) but by not applying the DSG to them, the executive has no legal basis for processing data of legal entities and thus cannot uphold Art. 5 and 36 BV[148], the legislator will add Art. 57j to Art. 57t of the Government and Administrative Act (*Regierungs- und Verwaltungsorganisationsgesetz* (abbreviated RVOG))[149] to provide for such a legal basis and thus implementing sufficient regulation concerning legal entities' privacy. In conclusion, legal entities will not enjoy protection under the nDSG anymore. However, they are protected under general regulation concerning compensation for privacy infringements.[150]

Data is considered "personal" if it relates to an identified or identifiable[151] person. Art. 3 item b oDSG contains the definition of **data subject**, which covers natural persons or legal entities whose data is processed. Art. 5 item b nDSG again is almost identical to the previous provision, but emphasizes that under the nDSG, it may only be a natural person that can be subject to data protection rights. The original draft of the nDSG included the possibility for heirs to exercise rights of the data subject in order to achieve a **"digital death"** of the deceased, especially in context with social media.[152] A comparable rule in the old law – stating that access to data of a deceased person must be granted if the applicant can prove legitimate and prevailing interest – can only be found in Art. 1 para. 7 oVDSG, specifying modalities of the right to information. The problem that this regulation had no legal basis in the oDSG would have been fixed if it were moved to the statutory level directly in the nDSG.[153] However, this instrument has not made it into the final version of the nDSG.[154] Even a counterpart to Art. 1 para. 7 oVDSG cannot be found in the E-VDSG anymore. The legislator has bowed to the critics of this concept whose main arguments were that the GDPR does not know an equivalent provision, it would cause disproportionate administrative effort and that the Swiss legal concept of privacy does not know a corresponding concept of personality rights *post mortem*.[155]

---

[146] Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 439; SVP, 'Eröffnung des Vernehmlassungsverfahren: Antwort der Schweizerischen Volkspartei (SVP)' (4 April 2017) 2.

[147] Christian Drechsler, 'Plädoyer für die Abschaffung des Datenschutzes für juristische Personen' (2016) 11(1) AJP 80-88, 85 et seq.; George (n 139), 20 et seqq. with further proof.

[148] Legal reservation. *C.f.* Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7118 et seq.

[149] Government and Administration Organisation Act.

[150] See on recovery of damages following breaches of privacy *infra* C.III.4.a.

[151] See, concerning the inherent relativity of the notion of identifiability, Rudin (n 121) 34 et seq.

[152] Eidgenössisches Bundesamt für Justiz, 'Vorentwurf nDSG' (n 5) 54; Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7044 et seq.

[153] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7044.

[154] An Art. 16 of the early draft held provisions about data of deceased persons.

[155] Eidgenössisches Bundesamt für Justiz, 'Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz: Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens' (10 August 2017) 26 with further proof.

3. Reception and Recipients

Special regulation for non-profit/non-commercial actors; the public as a legal recipient; use of public data; size-based obligations for companies; differentiation between recipients and third parties (especially within company groups); differentiation between local and international action; outsourcing options.

Even though both the old and the new DSG, know definitions of the receiving party[156], the regulation of unlawful data processing[157] links to "anyone who processes personal data".

IT outsourcing under the nDSG is addressed under the concept of the *Auftragsbearbeiter* or "**processor**" defined in Art. 5 item k nDSG. Among other rules, Art. 9 nDSG regulates IT outsourcing by giving the possibility of using a data processor where the appointing controller would be allowed to process the outsourced data (para. 1 item a) and there is no contractual or statutory confidentiality obligation (para. 1 item b). Additionally, the controller must ensure that the processor can maintain sufficient data security (para. 2) and the disclosure to third parties is prohibited unless the controller allows otherwise (para. 3).

The only provision for outsourcing in the oDSG can be found in Art. 10a oDSG which contains provisions if data is processed by third parties. Without using the term of "processor", this provision achieves the same regulation as under Art. 9 nDSG except for Art. 9 para. 3 nDSG, which regulates a system of chained responsibility.

The nDSG contains a sectoral **size-based restriction** in Art. 12 lit. 5 nDSG which allows the Federal Council to create exceptions from maintaining a record of processing activities for businesses with under 250 employees when the risk of privacy violation is low within this organisation. This was (or will be) acted upon in Art. 26 E-VDSG[158] generally exempting individual private persons and businesses with less than 250 employees unless sensible data is processed on a wide scope or high-risk profiling[159] occurs. Such size-based restrictions cannot be found in the oDSG.

Data made public (in the words of the DSG "made generally accessible" by the data subject) has a partially special set of rules under both the old and new DSG. Art. 6 para. 2 item f oDSG allows for easier cross-border data transfer if the data is made public. More importantly, Art. 12 para. 3 oDSG states the general rule (implying exceptions to this[160]) that a private actor does not violate the data subject's personality by processing data made public **without an explicit objection** by the data subject. Conversely for public organs, Art. 17 para. 2 item c oDSG (for processing sensitive data and personality profiles) and Art. 19 para. 1 item c oDSG (for further disclosure) state an element of permission if the data is made public. This does not change under the nDSG.

Whether and how a "**corporate privilege**" should be introduced in the nDSG was greatly discussed. Now, however, this is only found in a few provisions,[161] the most important of these Art. 31 para. 2 item b nDSG. It states that, in order to

---

156 Be it the data file under Art. 3 item g oDSG or the controller under Art. 5 item j nDSG. See on these definitions *supra* C.II.1.

157 See Art. 12 para. 1 oDSG and Art. 30 para. 1 nDSG.

158 If this provision will make it to the final form of the VDSG remains to be seen, see on the general controversy concerning the E-VDSG *supra* A.I. N 6.

159 See on the definition of high-risk profiling *supra* C.II.1.

160 The public disclosure must be made with the knowledge and will of the data subject, *i.e.* they must also have expected it to be publicly perceptible, *c.f.* Wemelinger (n 109) 169.

161 Lukas Bühlmann and Michael Reinle, 'Neues Schweizer Datenschutzrecht: Wichtigste Regelungen Der DSG-Revision Im Überblick' *mondaq* (9 December 2020) <https://www.mondaq.com/privacy-protection/1014308/neues-schweizer-datenschutzrecht-wichtigste-regelungen-der-dsg-revision-im-berblick> accessed 25 March 2022.

commercially compete with other businesses, the controller may process data for this purpose if they do not disclose the data to third parties. Other entities within the same company group, however, do not count as third parties under this provision, thus, the sharing of acquired personal data within company groups is made easier.

Additionally, the controller's obligation to provide information (under Art. 20 para. 4 nDSG or – in case of the data subject invoking his right to information – Art. 26 para. 3) are eased for disclosure within such company groups.

In the oDSG, explicit corporate privileges cannot be found. Such privileges could only be found in interpretation of Art. 13 para. 2 item b oDSG,[162] which the legislator explicitly left to be resolved by jurisprudence.[163] As can be seen, the legislator refrained from this room for interpretation in Art. 31 para. 2 item b nDSG.

III. Relationship between Discloser and Recipient

1. Provisions for Disclosure

Does regulation exist? personal data as intellectual property and commercial good; data law as a framework for action; „informational self-determination".

"**Disclosure**" as meant in the context of this report (the individual (data subject) voluntarily giving data concerning him- or herself to another person (controller)) is not *per se* defined in the old and new DSG. It only knows the (not entirely fitting) term of *bekanntgeben*[164] in Art. 3 item f oDSG,[165] which means as much as giving others knowledge of own or other people's personal data,[166] which is one of the variants of "processing" (*bearbeiten*) as enumerated in Art. 3 item e oDSG. Closer to the concept of disclosure as used in this report would be the term *beschaffen*, which can be translated to "acquire" and which is used as an example for the definition of processing in both the old and new DSG.[167] However, one should note that *beschaffen* refers to the opposite perspective, *i.e.* that of the controller actively acquiring data. This term appears as a trigger for information obligations[168] and is not described any further by law. However, as can be seen in Art. 14 para. 1 oDSG[169], data can also be "acquired" from a third party. Therefore, this definition also does not fully resemble the definition of "disclosure" in the context of this report.

In conclusion, "data disclosure" (which can be understood to be a form of "processing") between private actors is, as a general rule, always allowed and only restricted (or even prohibited) where regulated in the DSG (permission subject to prohibition), for both new and old DSG do not follow the approach of a **prohibition subject to permission**.[170]

The concept of **informational self-determination**, developed by the German Federal Constitutional Court[171], has made its

[162] One can argue that a "third party" in competition contexts would not include entities in the same company group.

[163] Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 461. However, a corporate privilege was not picked up in practice under the oDSG, *cf.* only EDÖB, 'Zentralisierung von Human Resources im Ausland' (3 June 2022) <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/18--taetigkeitsbericht-2010-2011/zentralisierung-von-human-resources-im-ausland.html> accessed 3 June 2022; Schweizerische Lauterkeitskommission SLK, 'Entscheid Nr. 179/16' (23 November 2016) N 9.

[164] See *supra* C.I.

[165] Art. 5 item e nDSG.

[166] Rudin (n 121) 43.

[167] Art. 3 item e oDSG / Art. 5 iten d nDSG.

[168] Art. 14 and 18a oDSG / Art. 19 nDSG.

[169] Art. 19 para. 1 nDSG.

[170] See on this *supra* C.I.

[171] *Volkszählungsurteil* [1983] 1 BvR 209/83, [1984] 37 Neue Juristische Wochenschrift 419 (BVerfG).

way into the Swiss legal discourse, being prominently cited in the reasoning for the first draft of the DSG[172] in 1988. It was later taken over by the Federal Supreme Court[173] (which reads this fundamental right – against the wording of a "right to protection against misuse" – as a civil liberty[174] under a conjunction of Art. 10 para. 2 and 13 para. 2 BV) in its arguments. Informational self-determination can be seen as a form of **legal transplant**[175] that pervades the Swiss data protection law as matter of protection, best seen in the centrality of the concept of the "personality violation".[176]

a. Disclosure Prohibitions

Protections of secrecy; multi-referentiality; disclosure to actors abroad; communication towards the public.

As a general rule, Art. 4 para. 1 oDSG[177] prohibits the processing of data if it violates another law (such as confidentiality under banking law, trade secret law etc.). However, the prevailing view among legal scholars (concerning the oDSG) requires additionally that the violated law must at least also – directly or indirectly – **intend the protection of a person's privacy**.[178] While dissenting voices, notably the EDÖB, take a broader viewpoint[179], it is widely regarded as insufficient that such a violation arose from an unlawful purpose.[180] This is a notable difference from the GDPR, for the DSG – in contrast to Art. 5 para. 1 item b) GDPR – speaks nowhere of the legitimacy of the purpose. Therefore, the interpretation of Swiss data protection law cannot be aligned to an European understanding.[181] This is true for both the old and new DSG, thus adherence to this interpretation can be assumed.[182]

Regulation that (also) intends the protection of privacy can be found in various areas of Swiss law, such being trade secrets, releases from confidentiality or the (historically prominent)[183] concept of banking secrecy. For example, Art. 47 of the Banking Act (*Bundesgesetz über die Banken und Sparkassen* (abbreviated BankG)) includes a criminal provision protecting the **secrecy of banking**, a norm criticized in connection to the "Suisse Secrets" revelations as criminalizing journalism related to data leaks.[184]

Whether the violation of other provisions of the DSG – in addition to their respective legal consequences – leads to unlawful processing

---

[172] There only as „self-determination concerning one's personal data", *cf.* Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 459; however, the legislator now fully acknowledges the right to informational self-determination in this wording as matter of protection, see Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7010.

[173] *Cf.* only 140 I 2, [2014] (BGE) E.9.1 et seqq. with further proof.

[174] Stefanie-Daniela Waldmeier, 'Informationelle Selbstbestimmung - ein Grundrecht im Wandel?' (University of Zurich 2015) 104, 160.

[175] Concerning the term "legal transplant", refer to the discussion at Gebhard M Rehm, 'Rechtstransplantate als Instrument der Rechtsreform und -transformation' (2008) 72(1) The Rabel Journal of Comparative and International Private Law 1.

[176] See on the term of personality violations and the concept behind it *supra* C.I.

[177] Art. 6 para. 1 nDSG.

[178] *Helsana*+ A-3548/2018, [2019] (BVGer), E. 5.4.3 with further proof; Bühlmann and Schüepp (n 103), 6; David Rosenthal and Yvonne Jöhri, *Handkommentar zum Datenschutzgesetz* (Schulthess 2008) Art. 4, N 6.

[179] EDÖB, 'Empfehlung des EDÖB betreffend Bonusprogramm Helsena+ der Helsena Zusatzversicherungen AG' (Bern 26 April 2018) A2018.04.13-0001 4 et seq.

[180] *Helsana* (n 178) E.5.4.4; Bühlmann and Schüepp (n 103), 43.

[181] Bühlmann and Schüepp (n 103), 6.

[182] So too *Helsana* (n 178) E.5.4.3.

[183] Stefan Tobler, 'Warum die Schweiz ihr Bankgeheimnis verlor' in Mark Eisenegger, Linards Udris and Patrik Ettinger (eds), *Wandel der Öffentlichkeit und der Gesellschaft: Gedenkschrift für Kurt Imhof* (Springer Fachmedien Wiesbaden 2019).

[184] Isabel Pfaff, 'Suisse Secrets: Wie die Schweiz auf die Enthüllungen reagiert' *Süddeutsche Zeitung* (21 February 2022) <https://www.sueddeutsche.de/wirtschaft/suisse-secrets-schweiz-credit-suisse-bankgeheimnis-1.5533261> accessed 26 March 2022.

under Art. 4 para. 1 oDSG[185] (and therefore to a violation of personality under Art. 12 para. 2 item a oDSG[186]) is not quite clear.[187] It is clear, however, that the violated provision of the DSG must intend the protection of individual privacy in order to trigger Art. 4 para. 1 oDSG.[188] As the whole DSG intends the protection of personal privacy (Art. 1 DSG), it would seem only consequential to assume a violation of the principle of legality if any provision of the DSG is breached.[189] While not all scholars follow this reasoning,[190] it appears settled amongst a majority of scholars that at least the rules directly concerning the acquisition and processing of data must be included under Art. 4 para. 1 oDSG.[191] Not included would therefore be, *inter alia*, violations of the rights of the data subject or the obligation to register processing activities.[192] Advocates of this view argue that as it not only allows for a delimitation from the traditionally more strictly regulated public sector (which is bound to law and order qua the rule of law anyway[193]), it also takes into account the fact that Art. 12 para. 2 item a oDSG only refers to certain principles (such as Art. 4 para. 1) and thus does not sweepingly want to constitute the violation of any norm of the DSG as a violation of personality.[194] The violation of a provision of the DSG can, however, lead to **processing violating the principle of good faith** in individual cases and thus violate the principle in Art. 4 para. 2 oDSG.[195] Therefore, the question whether a provision shall (also) protect privacy must be answered restrictively for provisions of the DSG, so that only **rules directly concerning the data processing** are included.

Particularly important for the nDSG in this respect are the newly added information obligations, which do not concern processing itself and therefore missing information cannot constitute a violation of Art. 6 para. 1 nDSG.[196]

Art. 35 oDSG protects against a "breach of professional confidentiality" and penalizes the wilful disclosure of secrets[197] and sensible data obtained while practicing one's profession and therefore necessarily encountering said data. The standard of protection of such secrecy was increased[198] in the nDSG, of which Art. 62 now allows for a penalty of **up to 250.000 Swiss francs**, while the previous limit was 10.000 Swiss francs (Art. 333 para. 3 in conjunction with Art. 106 para. 1 of the Swiss Penal Code (*Schweizerisches Strafgesetzbuch* (abbreviated StGB)).

However, the major novelty of the new Art. 62 para. 1 nDSG is that it is now not only applicable for sensitive data, but for all secret

---

185 Art. 6 para. 1 nDSG.

186 Art. 30 para. 2 item a nDSG.

187 Bühlmann and Schüepp (n 103), 43.

188 ibid.

189 Bruno Baeriswyl, 'Art. 4' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 52.

190 Rosenthal and Jöhri (n 178) Art. 4 N 9.

191 Bühlmann and Schüepp (n 103), 42.

192 ibid.

193 As common in civil law, the principle of legality as (sub-)principle of an overarching rule of law in a formal sense requires all state authorities to base their actions on written law, which can be seen in Art. 5 para. 1 BV, *cf. Egli (n 14) 26*.

194 Art. 12 para. 2 oDSG refers to some acts as being "especially" (*insbesondere*) prohibited, which could allow for the interpretation that comparatively minor violations do not automatically lead to a personality violation, Art .12 para. 1 oDSG.

195 Baeriswyl, 'Art. 4' (n 189) 53.

196 Identical in content to Art. 4 para. 1 oDSG.

197 The definition of "secrecy" is the same as under Art. 321 StGB: the information must not be commonly known and the data subject must have a reasonable interest in keeping the secrecy, see Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 72 et seq.

198 See on the intensification of professional confidentiality *infra* C.IV.3.d.

data, thus creating a **professional duty of secrecy in any professional situation**.[199]

b. Disclosure Obligations

Identification obligations and prohibition of anonymity; tax and other control.

Explicit obligations to disclose data can especially be found in Art. 42 paras. 1 and 2 of the Tax Harmonisation Act (*Steuerharmonisierungsgesetz,* abbreviated StHG) requiring the taxpayer to disclose all data relevant for assessing their **taxation**, or in Art. 40 ZGB in conjunction with the Ordinance on the Civil Status (*Zivilstandsverordnung,* abbreviated ZStV), which obliges every resident to notify about the data necessary for the maintenance of a **civil status register** (this data is listed in Art. 8 ZStV). Somewhat corresponding to the latter, other disclosure obligations in context with the maintenance of registers exist for the commercial register (*cf.* for example Art. 62 ZGB) or the land register (*cf.* Art. 11 and 12 of the Ordinance on the Land Register (*Grundbuchverordnung,* abbreviated GBV).

There are some *de facto* disclosure obligations for the data subject under the guise of processing obligations: For example, Art. 3 of the Anti-Money Laundering Act (*Geldwäschereigesetz,* abbreviated GwG) obligates financial intermediaries (*i.e.* banks or other asset management companies) to verify the identity of the customer when establishing a business relationship. Conversely, this means for the customer that they need to disclose their relevant data for identification in order to conclude a contract with the financial intermediary – something that is all but inevitable in today's society. A similar construction can be seen in Art. 29 et seqq. of the Federal Act on Consumer Credit (*Bundesgesetz über den Konsumkredit,* abbreviated KKG) when it comes to credit assessment.

c. Voluntary Disclosure

Protection in dependency and hierarchy contexts; access to alternatives; prohibition of coupling; voluntary commercialization of personal data; Incentives to data disclosure and protection therefrom (protection of adolescents; competition law; nudging); prerequisites for consent; „privacy fatigue"; peer pressure (e.g. WhatsApp).

Art. 4 para. 5 oDSG[200] specifies on **consent**, which must be given in an **informed** and **voluntary** manner. Art. 6 para. 6 nDSG adds that consent must be given **for specific cases**, which is found only rarely in the oDSG (*cf.* Art. 6 para. 2 item b; Art. 19 para. 1 item b oDSG). "Specified" (or "individual") cannot be understood in a quantitative[201] but qualitative manner, meaning that the clear description of an adequate precise "case" for which consent shall be given is sufficient.[202] Thus, the consenting data subject should be able to easily identify the circumstances of future processing.[203]

Furthermore, Art. 4 para. 5 oDSG requires **express** consent when sensible data or personality profiles are processed. This marginally changed in Art. 6 para. 7 nDSG, which replaces personality profiles with high-risk profiling by private actors (item b) and "normal" profiling by public actors (item c), implying that voluntary disclosure is more strictly regulated in the public sector. A declaration is expressly given when it consists of written or spoken words or signs and thus directly shows the expressed intent.[204]

---

[199] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 72. See on professional secrecy again *infra* C.IV.3.d.

[200] Now a little more precise in Art. 6 para. 6 and 7 nDSG.

[201] Nonetheless, the BVGer, in *Helsana* (n 178) E.4.8.4, argues, that consent must be acquired for every act of disclosure to take personal privacy into account to the largest extent.

[202] Bühlmann and Schüepp (n 103), 16.

[203] Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 470.

[204] 121 III 31, [1995] (BGE) E.2c.

"Expressly" arguably[205] refers to both the form of expression and the content.[206]

Whether or not consent is given expressly when **included in terms and conditions** is disputed amongst legal scholars in Switzerland.[207] In general, it can be assumed that consent may only be considered to be expressly given if – by clicking the box of confirmation – the data subject can reasonably foresee (under consideration of the so called "**rule of unusualness**" in Swiss GTCB[208] law) that concrete processing requiring consent will occur.[209] If this requirement is met, a confirmation procedure via opt out (the box is checked from the outset) is also possible under Swiss law.[210]

Swiss Courts[211] to some extent understand a **prohibition of coupling**[212] to exist in Art. 4 para. 5 oDSG, which stipulates that consent must also be given **voluntarily**.

However, this cannot be compared to a prohibition of coupling as it is discussed for Art. 7 para. 4 GDPR; some might therefore argue that Swiss data protection law does not have a prohibition of coupling.[213] In any case, what does exist is the case law ruling that a disadvantage obtained where refusing consent can only lead to an otherwise involuntary consent if said disadvantage has no connection to the purpose of the sought data processing whatsoever, or if the disadvantage is heavily disproportionate to the purpose.[214] An example for this can be found in a ruling of the Federal Administrative Court[215] concerning a public swimming facility which used biometric data to sell its season tickets. The price for single tickets which could be purchased without giving biometric data was many times higher. The court ruled that the consent required for obtaining this biometric data was involuntary because the alternatives[216] to the disclosure were unreasonable and the fact that one must pay a higher price for not disclosing biometric data had an insufficient connection to the disclosure (however, the latter point was not made explicit by the court). It should be noted that this view is not undisputed.[217]

While the oDSG is largely silent on matters protecting voluntary disclosure – except for provisions on consent, see above – the nDSG, in its Art. 7 para. 3, states that the "controller is obligated to ensure by means of establishing suitable pre-sets that processing of personal data is restricted to the minimum necessary for the purpose of processing, insofar as the data subject does not determine

---

[205] This is disputed in literature, see for another opinion: Rosenthal and Jöhri (n 178) Art. 4, para 83.

[206] David Vasella, 'Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht' [2015] Jusletter, 16 <https://jusletter.weblaw.ch/juslissues/2015/824/zur-freiwilligkeit-u_90937b2cfa.html>.

[207] Bühlmann and Schüepp (n 103), 31, 37.

[208] Abbreviation for general terms and conditions by businesses.

[209] Vasella, 'Einwilligung im Datenschutzrecht' (n 206) 15 et seq.; See also for more detail on this „rule of unusualness" in Swiss GTCB law *infra* V.IV.1.d.

[210] A-3908/2008, [2009] (BVGer).

[211] *Cf. Helsana* (n 178) E.4.7.

[212] "Coupling" under this meaning is understood as the connection between consent and a conclusion of contract which does not necessarily require data processing.

[213] Bühlmann and Schüepp (n 103), 11.

[214] *Helsana* (n 178) E.4.7; Schweizerischer Bundesrat, 'Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung' (2003) 154(10) Bundesblatt 2101, 2127.

[215] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 12 et seq.

[216] *Cf.* Vasella, 'Einwilligung im Datenschutzrecht' (n 206) 16, who explcitly connects voluntariness and reasonable alternatives.

[217] *Cf.* only Bühlmann and Schüepp (n 103), 12 et seq. with further proof.

otherwise"[218] – this would *de facto* mean a consent requirement in cases of "excessive" collection of personal data, however, as the purpose is determined by the controller, this could prove to be very unspecific and broad in practice.

Notable in this respect are different **opt-out regulations** in the oDSG which remain largely unchanged in the nDSG. The possibility to opt out is always paired with publicised data. Further, processing of all data can be explicitly prohibited by the data subject as can be seen in Art. 12 para. 2 item b oDSG,[219] which defines a violation of personality as processing against the explicit will of the data subject and thus giving them a general right to opt out.[220]

Regarding the **protection of adolescents**, the general rules of Swiss law concerning declarations of will for concluding a contract apply. This means that a minor can consent to processing of their personal data where they have a "sense of judgement" according to Art. 19c ZGB, which is generally assumed at the age of 13.[221]

2. Recipient Obligations

a. Requirements for Personal Data Reception

Information; requirements concerning content and formalities; warnings; notifications; assurances.

Transparency was already a fundamental principle under the oDSG (Art. 4 para. 4 oDSG) and is now intended to be sharpened under the nDSG.[222] The legislator implemented **further information obligations** to be assessed in this section. Having the goal in mind that transparency and in the following the data subjects' rights and personal responsibility shall be strengthened, it comes as a surprise that Art. 4 para. 4 oDSG[223] was cut and only incorporated into Art. 6 para. 3 nDSG insofar as the purpose of processing must be recognizable. The requirement for the act of processing itself to be recognizable is only found in the general information obligation (Art. 19 nDSG). This might seem like no downgrade to the level of privacy protection, but, in fact, it would mean that the failure to inform that data is processed altogether allows for certain administrative remedies by the EDÖB[224], but arguably[225] constitutes no privacy infringement as no principle under Art. 6 nDSG was violated. To fix this contradiction to the regulatory goal, a basic amount of transparency could be read into the good faith principle of Art. 6 para. 2 nDSG: To match the (eliminated) obligation in Art. 4 para. 4 oDSG under the nDSG, data processing that is not recognizable as such will therefore always be considered as being against good faith and in violation of the principle of Art. 6 para. 2 nDSG.[226]

Art. 14 oDSG contains a specific obligation for **controllers of data files to inform** affected persons in case of the collection of sensitive personal data and personality profiles. But the collection of data is only one of multiple acts of processing on the side of the data file controller; what they do with this collected data does not trigger Art. 14 oDSG.[227] This obligation exists also in cases of acquisition of such data from third parties. However, if the data is acquired from

---

[218] See on this privacy by default approach in more detail *infra* C.IV.2.a.

[219] Art. 30 para. 2 item b nDSG.

[220] Bieri and Powell (n 86), 6.

[221] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 13.

[222] See on the goals of the revision *supra* A.I.

[223] Principle of recognizability of data processing as well as its purpose.

[224] See on the enforcement powers of the EDÖB *infra* C.IV.3.a.

[225] Information obligation do not concern the data processing itself and are therefore arguably not included by the principle of legality, see *supra* C.III.2.a.

[226] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 15.

[227] Amédéo Wermelinger, 'Art. 14' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 189 et seq.

such third parties, belated information at least until when the data is stored or if the data is not stored, on its first disclosure to a third party is possible (para. 3). Otherwise, the information must be given at the same time the collection occurs.[228] Para. 2 contains the **minimum contents** of such information (identity of the controller, purpose, and categories of data recipients). These minimum contents are non-exhaustive, which constitutes a "Swiss Finish" not giving companies clarity on how much information exactly they must provide. The resulting overcompliance might result in an informational overload and would therefore not be in the name of transparency.[229] This "Swiss Finish" remains in the nDSG. The legislator reasons this regulation with the necessity of flexibility because the DSG addresses a vast variety of different types of data processing.[230] Stipulating non-exhaustive minimum requirements enables companies (in theory) to give only information that they deem necessary for promoting transparency and data subject rights; they would not be obliged to disclose information that surpasses this purpose in the individual case. Art. 14 para. 4 oDSG contains comprehensive restrictions to the information requirements (a) where "collection or disclosure of data is specifically provided for by law" and (b) where "such information is not possible or possible only with disproportionate effort". To prevent evasion by invoking disproportionate effort and in regard to the worthiness of protection of sensible data and personality profiles, this exception is read by various legal scholars restrictively and does not concern only anticipated difficulties in communication and rather needs more justification effort.[231] Para. 5 refers to Art. 9 paras. 1 – 4 oDSG, stating that the controller of a data file may refuse, restrict, or defer the information under the prerequisites mentioned there (these are the general restrictions of the right to information[232]).[233]

In the nDSG, Articles 19 to 21 deal with new **information obligations**, with Art. 19 setting the basic requirements, Art. 20 containing exceptions and restrictions to these requirements and Art. 21 dealing with the more specific topic of information on automatic decision-making. At their heart is the general provision in Art. 19 para. 1 nDSG, which states that the controller must inform the data subject of the acquisition[234] of personal data in an appropriate manner; this information obligation exists also where data is not acquired from the data subject. Similar to the oDSG, the information can be given belatedly under para. 5 – *in concreto* within one month after acquisition from a third party or (if earlier) until disclosure[235] to third parties by the controller. Para. 2 of Art. 19 nDSG contains the minimum requirements of such information and states that the controller must inform the data subject of the information required to exercise their rights under the nDSG[236] as well as transparent processing. The minimum to achieve this being: identity and contact information of the controller (item a), the purposes of the processing (item b) and, where applicable, all recipients of further

---

228 *Cf.* Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7052.

229 David Rosenthal, 'Der Entwurf für ein neues Datenschutzgesetz' [2017] Jusletter, 36.

230 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7051.

231 Wermelinger, 'Art. 14' (n 227) 192.

232 *Cf. infra* C.III.3.a.

233 These are the general restrictions of the right to information, see *infra* C.III.3.a.

234 Note that this is not "processing", but only one act of it.

235 Disclosure as in the meaning under Art. 5 item e nDSG.

236 However, it does not explicitly require the controller to make the data subject aware of these rights.

disclosure (item c).[237] It must be noted that the purposes are – although not required – regularly described extensively to comply with the principle of purpose limitation to the largest possible extent.[238] Para. 3 requires the controller to additionally inform the data subject of the categories of processed personal data where the data is not acquired from the data subject (directly).

Art. 19 para. 4 nDSG contains additional requirements for information in case of cross-border transfers, thus triggering a (possibly) belated information obligation: It requires that the controller inform the data subject of the foreign country (or international organ) where data is transferred to, as well as certain information of the legal basis for such transfers. This provision was subject to some criticism, as it is in many cases not easy to determine exactly every country data is transferred to.[239] In an effort to mitigate this compliance burden, one could interpret that the naming of an identifiable country would be sufficient, thus it would be compliant to name "every country in the world", "Europe", "America", or similar.[240] If this interpretation will be transposed into practice despite not being intended by the legislator[241] remains to be seen.

Art. 20 para. 1 nDSG names situations where no information under Art. 19 must take place, for example where the data subject already has obtained the necessary information[242] (item a), or where processing is provided for by law (item b), or data is processed by the media for merely editorial purposes (item d), amongst others. Para. 2 states that no such information must take place in case of acquisition through third parties ("not from the data subject") and where such information is not possible (item a) or information requires disproportionate effort (item b).[243] Para. 3 enumerates circumstances where the controller may restrict, postpone, or refrain from complying with providing the information, amongst these where "prevailing third-party interests require such action" (item a), providing the information would frustrate the purpose of processing (item b) or in case of certain prevailing national security or law enforcement actions by a federal body (item d). Notable at this place is the "Swiss Finish" –which the Swiss information obligation rules are full of[244] – in Art. 20 para. 3 item c: The controller may restrict information if required by his overriding interest *and* he does not disclose data to third parties. In an earlier draft of the nDSG, the **corporate privilege** in Art. 20 para. 4 nDSG did not exist, which was later added due to criticism concerning overregulation of company groups.[245]

The scope of the information beyond the statutory minimum is determined in the individual case. As can be seen in Art. 20 para. 2 item b nDSG and in line with the underlining principle of proportionality in

---

[237] See for the crticism of this non-exhaustive phrasing (as "Swiss Finish" already above.

[238] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 38.

[239] Rosenthal, 'Entwurf des nDSG' (n 229) 36. For example Microsoft has for the purpose of IT-Outsourcing service providers (which again have sub-partners) all around the globe, *cf.* Vasella (n 70) 49:10.

[240] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 38.

[241] The reasoning in Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7052 does not give away this interpretation.

[242] Questionable how explicit such information must be obtained by the individual in question, or whether "making available", *e.g.* via privacy policy, is sufficient.

[243] The latter provision can, in practical application, allow for de facto non-applicability of information requirements in case of third-party acquisition of personal data, since the question of what is "disproportionate effort" is inherently flexible and violations are difficult to pursue as individuals will, precisely due to nonadherence to Art. 19 nDSG, not be aware of such violation. As the nDSG is not in force yet, it remains to be seen exactly how this will function in practice.

[244] *Cf.* only Rosenthal, 'Entwurf des nDSG' (n 229) 35 et seqq.

[245] ibid.

Swiss data protection law, the amount of information must comply with good faith and the principle of transparency.[246] It must not only **enable the data subject to act upon his or her rights** under the nDSG, but also **suffice for an informed decision** (Art. 6 para. 6 nDSG) from the perspective of an average person in the targeted audience[247], whereas both goals can be achieved separately. However, these abstract explanations show the weakness of this "Swiss Finish" to give precise compliance prerequisites to companies.[248]

Even though not explicitly provided for, the information must be **easily accessible and sufficiently visible**, whereby the principles of Swiss GTCB law apply.[249] The Federal Council intends to allow for an integration of the privacy statement into terms and conditions of a company (GTCB).[250] However, this would not comply to transparent visibility, especially under the consideration that an average consumer might not expect information relevant for data protection in general terms and conditions.[251]

Art. 21 para. 1 nDSG further requires controllers to inform data subjects of decisions taken on the basis of entirely automatic processing and which have legal consequence or substantial adverse effects for the data subject.

Art. 19 to 21 nDSG apply to both private and public actors. This is different under the oDSG, which holds an information obligation for private actors only if they process sensible data or personality profiles, Art. 14 oDSG. This contains – to the least – the identity of the person holding the data collection, the purpose of the processing and the categories of data recipients if further disclosure is intended.

Art. 18 to 18b oDSG hold information obligations for public actors. They apply if personal data is acquired by federal bodies and include more necessary information such as a reference to the right for information and the consequences if a data subject refuses to provide the required data.

b. Obligations Concerning the Handling of Received Personal Data

Purpose dedication/limitation; technological and organizational measures; data security; deletion and retention; further transmission and limitations thereto, also concerning transmission abroad.

Art. 4 para. 3 oDSG contains the principle of purpose limitation,[252] which regulates the scope of data processing by the controller. The only restriction – in both old and new DSG – for subsequent change of purpose by the controller is the **perceptibility of the change** and the **compatibility with the original purpose**:[253] A change of purpose is irrelevant for the legality of processing, if the new purpose is recognisable under the concrete circumstances or the data subject should have expected it in good faith.

The principle of data correctness (Art. 5 para. 1 oDSG) requires that the received data must be kept **correct and complete**.[254]

Art. 6 oDSG deals with **data transfer abroad** and also works around the concept of the violation of personality.[255] Even though an unlawful data transfer abroad is not labelled a

[246] Bühlmann and Schüepp (n 103), 18 et seqq.

[247] ibid 20 et seq.

[248] This criticism which also applies to the current DSG was already outlined earlier in this chapter.

[249] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7050.

[250] ibid.

[251] Bühlmann and Schüepp (n 103), 31; See further on this „rule of unusualness" *infra* C.IV.1.d.

[252] See on the principles *supra* C.I.

[253] Bühlmann and Schüepp (n 103), 44.

[254] See on the nature of correctness and completeness *infra* C.IV.3.c.

[255] Metille (n 62), 76.

violation of personality under Art. 12 para. 2, a violation of Art. 6 oDSG (which is a provision directly connected to the act of processing) leads to a violation of the principle of legality and thus a violation of personality under the DSG.[256] Para. 1 assumes such violations in the "absence of **legislation that guarantees an adequate level of protection**" for the country concerned. Assessing such legislation is the responsibility of the EDÖB,[257] who keeps a list of countries with an adequate level of data protection, *cf.* Art. 7 oVDSG.[258] A transmission of data to a country named on said list of the EDÖB leads to the rebuttable presumption according to Art. 3 para. 1 ZGB that the controller was in good faith and therefore cannot be held liable. The presumption, however, can be refuted if the controller has knowledge that the recipient cannot guarantee an adequate level of data protection *in concreto*.[259] In this case the controller commits a data protection breach even despite the existing "adequacy decision". The other way around, if a country is not listed as adequate, this does not necessarily mean that it does not have adequate data protection standards. Rather, controllers can assess the data protection standards of the third country in the individual case by themselves.[260] In these cases, a court can also decide on the adequacy of data protection in a third country. Aligning with the *Schrems II* decision of the ECJ,[261] the EDÖB recommends looking at the factual – not the written – situation of data protection law.[262]

Para. 2 of Art. 6 oDSG names the requirements for transferring personal data outside Switzerland in absence of an adequate level of protection, enumerating different possibilities, which are:

(a) sufficient guarantees, in particular standard contractual clauses;
(b) individual consent – this is logically subject to the consent requirements in Art. 4 para. 5;
(c) immediate connection to a contract and the data is personal data of contractual partner;
(d) safeguarding prevailing public interest or establishment, exercise, or enforcement of legal claims;
(e) for the protection of life or bodily integrity of a person;
(f) publication of data and no explicit prohibition of processing and
(g) disclosure within the same company group.

The EDÖB gives explicit advice on when guarantees suffice for Art. 6 para. 2 item a oDSG.[263] Its two core assessments are that (a) the controller must analyse the additional measures to be taken on the basis of the guarantee of the above mentioned[264] fundamental rights, closing identified gaps with **Standard Contract Clauses** (SCCs) and that (b) **Binding Corporate Rules** (BCRs) cannot fully replace SCCs. Additionally, the EDÖB states – in line with the ECJ judgement[265] – that contractual measures themselves do not suffice if the administrative law of the third country allows infringements of privacy by

256 See on the principle of legality *supra* C.III.1.a.

257 Zanon and Boccali (n 41).

258 There are 44 individual countries with adequate protection on this list as on November 2021. The EU as per se is not part of this list, see EDÖB, 'Stand des Datenschutzes weltweit' (15 November 2021).

259 Zanon and Boccali (n 41), 41.

260 EDÖB, 'Datenübermittlung ins Ausland' (n 41) 3.

261 *Schrems II* C-311/18, [2020] (ECJ). See on this not uncommon alignment to European decisions *supra* A.II as well as *infra* C.IV.3.b.

262 Zanon and Boccali (n 41).

263 EDÖB, 'Datenübermittlung ins Ausland' (n 41).

264 See on data protection relevant fundamental rights *supra* C.I.

265 *Schrems* (n 261); on the relevance of the adaption of this *cf.* Zanon and Boccali (n 41), 41, 43.

authorities against which the controller has no adequate form of remedy.[266]

This approach to the transfer of data abroad slightly changes under the nDSG (Art. 16 – 18). Art. 16 para. 1 nDSG stipulates, as a general rule, that data transfer is always allowed when the Federal Council acknowledges an adequate level of protection. Not only does this change the public body responsible for the adequacy decisions, but also allows for a legally reliable data transfer abroad, aligning with the concept of Art. 45 GDPR.[267] Art. 8 E-VDSG specifies some points to be considered while determining an adequate level of data protection addressing the Federal Council.[268] Those points are: international obligations in the field of data protection (item a), human rights (item b), legislation, relevant case law and enforcement of statutory data protection law (item c), guarantee of rights of the data subject (item d) and an effective supervisory authority (item e).

Where no adequacy assessment exists, Art. 16 para. 2 of the nDSG allows transfers due to an international treaty (a), data protection clauses in a contract of certain parties where notification of the EDÖB has occurred in advance (b), guarantees set by federal bodies (which, in practice should mirror the aforementioned document of the EDÖB concerning Art. 6 para. 2 item a oDSG[269]) (c), standard contractual clauses approved by the EDÖB in advance (d), and obligatory internal company rules approved by the EDÖB or by a competent authority in a country considered as having an adequate standard of data protection in advance (e). Furthermore, the Federal Council may approve other methods allowing for suitable data protection measures in cases of no existing adequacy decision, Art. 16 para. 3. This is implemented in the E-VDSG[270]: Art. 9 E-VDSG specifies guarantees as under Art. 16 para. 2 item b and c nDSG, Art. 10 E-VDSG refers to SCCs under Art. 16 para. 2 item d nDSG, and Art. 11 E-VDSG to BCRs under Art. 16 para. 2 item e nDSG. Additionally, Art. 12 E-VDSG opens the possibility of codes of conducts and programs of self-certification alike the former Swiss-US Privacy Shield.[271]

Furthermore, Article 17 nDSG allows for other situations where personal data may be disclosed abroad in cases where there is no adequate level of protection, these being largely similar to and only a little more specific than the ones in Art. 6 para. 2 oDSG. What is new is that the nDSG does not contain a privilege for company groups (previously Art. 6 para. 2 item g oDSG) anymore, meaning that cross border privacy protection is strengthened versus international players like Meta or Alphabet.

In certain situations, Art. 17 para. 2 provides that the controller or processor must inform the EDÖB of these cases upon request.

Article 18 nDSG stipulates that "where personal data is provided for the information of the public with automated means of information or communication and is made available to the general public, this is not considered disclosure abroad even when data are accessible from abroad". This merely

[266] EDÖB, 'Datenübermittlung ins Ausland' (n 41) 6.

[267] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 28 et seq.

[268] Art. 8 E-VDSG does not name an addressee, which is only one point of critique to the E-VDSG as a whole, see Wermelinger, 'E-VDSG' (n 6) 10. Therefore, contrary to aforementioned advice of the EDÖB, Art. 8 E-VDSG does not stipulate any obligation relevant to the individual controller.

[269] EDÖB, 'Datenübermittlung ins Ausland' (n 41).

[270] Please take note that, following the criticism of the E-VDSG, the extent of future changes remains unclear. However, the provisions mentioned here were not subject to overt criticism, which is why one might assume the final version of the VDSG would be reasonably similar. Please refer to *supra* A. I.

[271] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 30.

mirrors Art. 5 oVDSG – taken to statutory level by the revision – ruling that a **publication of personal data on the internet**, which is also accessible abroad, does not count as disclosure under Art. 16 para. 1 nDSG if it was disclosed for public information purposes. This is especially relevant for media.[272]

A recent change in practice concerning international data flow occurred when the ECJ nullified the EU-US Privacy Shield[273] in 2020. As a direct reaction, the EDÖB concluded that the US did also not meet the required guarantees of adequate protection under Swiss data protection law and therefore the **Swiss-US Privacy Shield** should be invalid.[274] This reaction of the EDÖB is a prime example of what *Bradford* – in her fundamental analysis of the international influence of European legislation, the "Brussels Effect" – identified as so-called "**copycat litigation**":[275] Replicating EU decisions (which are based on comprehensive regulation and respective investigative powers, as well as know-how) such as for the adequacy of other countries' data protection standards lifts the organisational burden to investigate and examine foreign legal systems of the EDÖB; especially, he – by free riding EU decisions – does not need to develop and argue his own legal construct on why US data protection law is not adequate (which *Bradford* describes as **"de jure Brussels Effect"**[276]).

Not only does the EDÖB follow the argument that contractual measures cannot protect from state intervention, see above,[277] but it can also be reasoned that the Swiss may fear about losing their own adequacy decision by the EU because under the Swiss-US Privacy Shield disclosure from Switzerland to a country with – from the perspective of the EU – no adequate data protection would be possible.[278] Since then, the US have been moved from the list of countries "with an adequate protection under certain circumstances" to the list of countries with "**insufficient protection**".[279] In conclusion, the rebuttable assumption that data transfer is generally possible to the US under the prerequisites of the Swiss-US Privacy Shield agreement can no longer be upheld.[280]

Art. 7 oDSG requires **adequate technological and organizational measures (data security)** for the protection of personal data held by the controller against unauthorized processing, with para. 2 referring to specified rules set by the Federal Council. This was acted upon in Art. 8 et seqq. oVDSG stating some obligation to install specified measures.[281] The systems of a person processing data should be reasonably protected against the risk of unauthorized or accidental destruction, accidental loss, technical errors, counterfeit, theft or unlawful use, and unauthorized change, copy, access, or other processing of personal data (Art. 8 oVDSG). Art. 9 oVDSG names concrete goals to apply to by implementing technical and organizational measures: these being (amongst others) control of access to personal data, control safe transfer of data, control of the identity of the persons to

---

[272] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7043.

[273] *Schrems* (n 261).

[274] EDÖB, 'Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG' (Bern 8 September 2020).

[275] There only for antitrust supervision Bradford (n 11) 122 et seqq.

[276] ibid 114, 123.

[277] EDÖB, 'Datenübermittlung ins Ausland' (n 41) 6.

[278] Anne-Sophie Morand and Selma Duc, 'International data transfers and the EU's adequacy decisions' [2021] Jusletter, 3, 24.

[279] EDÖB, 'Datenschutz weltweit' (n 258) 12.

[280] Zanon and Boccali (n 41), 42.

[281] It must be noted that according to the wording of Art. 7 para. 2 oDSG (and Art. 8 para. 3 nDSG) the VDSG can only stipulate "minimum requirements". Thus, the Federal Council is restricted in implementing too extensive measures.

whom data is disclosed to or control of the storage of personal data.

The provision of Art. 7 oDSG was largely retained in Art. 8 nDSG – para. 3 is basically identical to the previous para. 2. Para. 1 changes the wording from the passive, making it clear that under the nDSG, the controller and the processor are both responsible. Para. 2 of Art. 8 nDSG specifies on the scope of technical and organisational measures that "the measures must allow for the avoidance of violations of data security", with "violations of data security" explicitly defined in Art. 5 item h. nDSG as "a violation of security leading to unintended or unlawful loss, deletion, destruction, modification, disclosure or making available to third parties of personal data". This includes the unintended deletion of data or an e-mail sent to the wrong address; according to this definition, it is irrelevant whether the security breach is unlawful or intentional.[282]

Under the E-VDSG, Art. 8 para. 3 nDSG (concrete technical and organisational measures to guarantee data security) is specified in Art. 1 to 5 E-VDSG. Aligning with the risk-based approach of Swiss data protection law (outlined in Art. 7 para. 2 nDSG), technical and organizational measures must be permanently assessed according to their appropriateness taking into account purpose, means, scope and circumstances of data processing, potential dangers for individual privacy, the state of the art and costs of implementing such measures, *cf.* Art. 1 E-VDSG. Art. 2 E-VDSG sharpens the regulation of Art. 9 oVDSG by naming more goals and now requiring to "reach" these objectives – and not "take measures suitable to achieve"[283] them as it is ruled in the current law. This can be interpreted as heavy compliance obligation cast upon the user of information technology even though the developers should bear this obligation according to the newly adopted Art. 7 nDSG ("**privacy by design**"[284]).[285] Art. 3 to 6 E-VDSG contain obligations for protocolling of high-risk processing and for issuing a processing policy. This ordinance regulation seems quite distant from the opening clause in Art. 8 para. 3 nDSG which allows for specifying "data security" regulation and does not match with the narrow scope of the Federal Council powers to make legislation here (*cf.* "minimum requirements", Art. 8 para. 3 nDSG) and therefore is widely regarded as regulatory misstep.[286] This misstep of extensive executive regulation is criticized throughout the whole E-VDSG, which is why significant revision of it is to be expected before the nDSG enters into force.[287]

Concerning deletion and retention, Art. 6 para. 4 nDSG states that personal data must be destroyed or anonymised as soon as it is no longer necessary for the purpose of processing.[288] The oDSG knows – apart from remedies aiming at deletion, Art. 15 and 25 oDSG – no explicit rule for such deletion or more generally the end of the usage cycle of personal data. However, the principle of data correctness in Art. 5 para. 1 oDSG[289] contains the rule that (regarding its purpose) wrong or incomplete data[290] must be corrected or, if not possible, deleted.[291]

---

[282] Rosenthal, 'Entwurf des nDSG' (n 229) 24.

[283] Art. 9 para. 1 oVDSG.

[284] See on the privacy by design approach *infra* C.IV.2.a.

[285] Wermelinger, 'E-VDSG' (n 6) 7.

[286] ibid 8 et seqq.

[287] See on this criticism already *supra* A.I.

[288] This aspect of the principle of correctness is a novelty in comparison to Art. 5 para. 1 oDSG, who refers only to correctness (in relation to the purpose), but not necessity for the purpose, see *supra* C.I. and *infra* C.III.3.c.

[289] Art. 6 para. 5 nDSG.

[290] See *infra* C.III.3.c.

[291] Bieri and Powell (n 86), 5; Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7026.

Concerning the processing of personal data by federal bodies, Art. 38 nDSG states that prior to required deletion of the personal data these must make the personal data available to the Federal Archive, which decides whether the data are worthy of archiving.

3. Discloser Control

a. Transparency and Entitlement to Information

Art. 8 oDSG contains a **right to information** vis-à-vis controllers of data files, thus this right has a rather limited (personal) scope of application on paper compared to the new law. In practice however, the question whether the controller holds a data file or just "regularly" processes data in another way is largely ignored, as the term "data file" arose from a time where data was held in the form of card record systems. Nowadays, a data file is understood as any electronic storage and is therefore applicable in many scenarios of the modern age.[292]

Art. 8 para. 2 oDSG gives more detailed guidance exactly on the contents of the answer to an information request: the controller must **disclose all data held** in the data file plus its respective origin (item a) and purpose and if applicable the legal basis of the processing as well as the categories of processed personal data, parties involved with the data file and the recipients of said data (item b). Health data can only be accessed via an involved doctor, para. 3. Para. 4 stipulates that the holder of a data file stays obliged to grant access even if the held data is processed by a third party; *vice versa,* the third party is obliged to grant access if he cannot name the data file holder or if the holder is not resident in Switzerland. Because the right to information is a strictly personal right, the data subject cannot waive it in advance, Art. 8 para. 6 oDSG.[293]

Art. 9 oDSG deals with situations where the controller of the data file can refuse, restrict, or defer compliance with the right to information. In general, access can be denied if this is allowed by (formal) law (item a) or it is necessary to safeguard prevailing third-party interests (item b). Further, Art. 9 oDSG knows a differentiation between federal bodies and private actors: Federal bodies can also refuse, restrict, or defer information, if required by prevailing public interest, especially national security, or it contradicts the purposes of criminal investigations and other investigative measures, para. 2. Private actors, however, can deny access if required by own prevailing interest and they do not disclose concerned data to third parties (para. 4).

Art. 10 contains special ground for restriction of the right to information for certain publications published in the edited section of a medium publicised periodically, *i. e.* newspapers, in order to **protect journalists and their sources**. As long as access to data held by such media could identify sources, give insight into planned publications or endanger free formation of opinion, the controller can deny, restrict or defer access. This does only apply when concerned data is exclusively used in context of a publication of a journalistic work published in the respective part of the medium which is intended for editorial purposes.[294]

In the nDSG, Art. 25 to 27 deal with the data subject's right to information under the new law, which is (in general) similarly designed as the obligation to information (Art. 19 et seqq. nDSG[295]).[296] Para. 2 of Art. 25 contains the information that must be given to the data subject following such

[292] Rudin (n 121) 45 et seqq.; Rosenthal, 'Entwurf des nDSG' (n 229) 43. See on this already *supra* C.II.1.

[293] Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 452.

[294] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7070.

[295] See *supra* C.III.2.a.

[296] Rosenthal, 'Entwurf des nDSG' (n 229) 34.

inquiry. It must – in accordance to the regulatory goals of the nDSG[297] – contain information **to the extent necessary to maintain transparent data processing and to enable the data subject to exercise their other rights** under the nDSG.[298] These minimum requirements are to the least the identity and contact data of the controller (a), the processed personal data as such (b), the purpose of processing (c), the duration the personal data is held or, in case this is not possible, the criteria for the determination of this duration (d), the available information regarding the origin of the personal data where they were not obtained from the data subject (e), where applicable, the existence of an automated individual decision-making[299] (f), and where applicable, the recipients or categories of recipients to whom personal data is disclosed, as well as the information according to Art. 19 para. 4 nDSG.[300] These non-exhaustive minimum requirements raise the same questions on concrete and definite compliance obligations, already criticised concerning general information obligations.[301]

Art. 25 para. 3 allows for information about personal data pertaining to health by consent of the data subject to be given directly to a healthcare professional. Para. 4 clarifies that this information must still be provided even if processing is done via a processor, while para. 5 prohibits the waiver of this right in advance.[302] However, Art. 26 provides for several situations where the controller of the personal data may refuse, restrict, or defer compliance with the information request, most notably in cases provided by law, where a trade secret exists or on the basis of overriding third-party interests. Paras. 2 and 3 provide for further restrictions for private individuals and federal bodies. Of note especially is para. 2 item a, according to which the information may be refused, restricted, or deferred where processing occurred based on -legitimate interest and where no disclosure to third parties occurs. This is largely unchanged from the oDSG (Art. 9 para. 4 oDSG). Interestingly, companies within a company group are not considered to be third parties as of para. 3, thus allowing for "internal" use within company groups, which creates a "**corporate privilege**".[303]

An interesting peculiarity arises from Art. 26 para. 2 item c, where information can be rejected when the request is "**obviously trouble-making**" (*querulatorisch*), which can be understood as requests that aim towards a wilful (and apart from this purposeless) burdening or bothering of the controller.[304] However, following the principle that access can be applied free of reason, it can be reasoned that this exemption concerning the motivation of the request has a narrow scope of applicability.[305] This peculiarity can probably be traced back to often-criticized **misuse** in Swiss data protection practice, exercising the right to information for purposes alien to data protection law such as

---

[297] Strengthening of Transparency in a digitalised World, see *supra* A. I.

[298] See also 138 III 425, [2012] (BGE) E.5.3.

[299] Algorithms are used for this decision making. They are often protected by trade secret law. Therefore, the access to information can't contain the code or even parts of it, but only the "basic logics" the algorithm functions by, see Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7067.

[300] Information related to disclosure of personal data abroad, see *supra* C.III.2.a.

[301] See on this "Swiss Finish" and its criticism *supra* C.III.2.a.

[302] Because it is a personal right, see also Art. 8 para. 6 oDSG, above.

[303] *Cf.* on corporate privileges *supra* C.II.3.

[304] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 47.

[305] Griesinger (n 86), 44.

discovery[306] or access to relevant documents.[307]

Art. 27 nDSG copies the protection of media under the oDSG.

Transparency versus federal bodies is also improved by the obligation of the EDÖB to publish the register of processing activities of federal bodies, Art. 56 nDSG.

b. Co-Determination and Co-Decision Concerning Data Use

Restrictions for use; permission requirements; revocation of consent; contestation and objection; special rules for international contexts; technical requirements for the act of permission/consent.

As consent is not a predominant feature in Swiss data protection regulation[308], the **primarily intended tool of co-determination is the possibility to opt-out** from data processing as can be seen in both the old and new DSG in the special regulation for data intentionally made public, which has less prerequisites for processing, *e.g.* Art. 12 para. 3 oDSG, and, relating thereto, the option to always opt out from (and enter again into[309]) processing. Those opt-out mechanisms are found in Art. 6 para. 2 item f oDSG (transfer abroad of data made public), Art. 12 para. 2 item b, para. 3 (general processing by private and public actors) and Art. 19 para. 4 item a oDSG (disclosure of data made public by federal bodies). This stays the same under the nDSG.

The possibility to **revoke consent** per express declaration – which is a natural consequence of an opt-out approach – remains unchanged in the old and new DSG.[310] Despite not being regulated explicitly, it is seen as part of the voluntariness of consent in Art. 4 para. 5 oDSG[311] to be able to revoke given consent at any opportunity.[312]

Art. 21 para. 2 nDSG gives data subjects – subject to para. 3 – the right to express their position on **automated decisions** and the right to require review of such decisions by a natural person, thus allowing for some control over data use.

Against private actors, the data subject can enforce a prohibition of certain processes or the disclosure to third parties via claim, Art. 32 paras. 2 item a) and b) nDSG[313]. Furthermore, in Art. 37 nDSG[314] the data subject is given a right to **object to "disclosure"**[315] of personal data against (only) federal bodies. To do so, they must be able to demonstrate legitimate interest in this regard, unless an obligation to disclose exists[316] or the fulfilment of public duties is

---

306 Note that pre-trial discovery as known from US law is not known to Swiss law, which only has precautionary taking of evidence (Art. 158 of the Swiss Civil Procedure Code (*Schweizerische Zivilprozessordnung* (abbreviated ZPO))), which cannot be compared to pre-trial discovery (Laurent Killias, Michael Kramer and Thomas Rohner, 'Gewährt Art. 158 ZPO eine "pre-trial discovery" nach US-amerikanischem Recht' in Franco Lorandi and Daniel Staehelin (eds), *Festschrift für Ivo Schwander* (DIKE 2011) 948) and thus is no justifiable motivation for invoking a right to access of information under the DSG.

307 Rosenthal, 'Entwurf des nDSG' (n 229) 42 et seqq.; Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7066.

308 See on system nudges towards consent, its legal effects, and further details *supra* C.I. and C.III.1.c.

309 Schweizerischer Bundesrat, 'Botschaft zum oDSG' (n 67) 459.

310 Bühlmann and Schüepp (n 103), 41; Rosenthal, 'Entwurf des nDSG' (n 229) 15; Bieri and Powell (n 86), 7.

311 Art. 6 para. 6 nDSG.

312 Jutta S Oberlin and Rainer Kessler, 'Daten: Die Schlüsselrolle im Kampf gegen die Coronavirus-Pandemie?' [2020] Jusletter, 12; Bieri and Powell (n 86), 7.

313 This is a non-exhausting list, which also exists – although with slightly different examples – in Art. 15 para. 1 oDSG.

314 This norm does also exist – with slightly different wording – in Art. 20 oDSG.

315 This is not "processing", but the further transmission of personal data of the data subject by the federal body, see *supra* C.III.2.b.

316 See exemplary on disclosure obligations *supra* C.III.1.b.

jeopardized. If the federal body can prove that the objection had the sole purpose to deny enforcement of legal claims or assertion of legitimate interest, personal data can be disclosed despite the objection, Art. 36 para. 2 item e nDSG, thus relativizing the options for co-determination vis a vis federal bodies.[317]

c. Revocation

Data portability; deletion; „right to be forgotten / to forget".

A general right to deletion under the oDSG can only be derived from Art. 5 para. 2 oDSG – the **right to correct data**.[318] However, this is only applicable for the replacement of (partially) wrong data alongside the addition of incomplete data.[319] In cases of violation of personality,[320] the possibility to **sue** private actors according to Art. 28, 28a and 28l ZGB is opened by Art. 15 oDSG, which amounts to a right for deletion of privacy-infringing (= unlawfully processed) data. Apart from this, the oDSG does not contain a right to data portability or other means of revocation.[321]

However, Swiss courts developed a "**right to be forgotten**" in the context of Art. 28 ZGB as early as 1983, ruling that part of rehabilitating former criminals is that anyone "should be forgotten in a manner according to a natural course of events".[322] Whether this is the case must be decided in a weighing of interests foremost between the right to privacy on one side (that the concerned data is true does not hinder a violation of personality[323]) and the public interest for information on the other side. Even though this jurisdiction was developed for the ZGB, not the DSG, Art. 28 ZGB is in terms of a violation of personality and its justification identical to Art. 12 et seq. oDSG[324] and can therefore easily be upheld for data protection law in cases of unlawful privacy infringements.[325] Its *de facto* implementation can be found in Art. 12 para. 2 item b oDSG[326]: If the data subject explicitly prohibits processing, processing of data constitutes a violation of personality and is subject to justification. Consequently, this right for deletion (or to be forgotten) is not absolute and does not exist in situations where the violation of personality is justified under Art. 13 oDSG,[327] for example, when the processing is allowed by law.[328] Such rights (or duties) to preserve data may arise from tax, commercial or social security law.[329] That the concept of a right to be forgotten developed for the ZGB should be upheld for the new data protection law is also shown in Art. 32 para. 2 item c nDSG, which can be read as textualization of said jurisdiction.[330]

This approach to revocation changed in the nDSG only insofar as that the **right of rectification** is now separately provided for in Art. 32 para. 1 nDSG. This change has a surprisingly high impact: Under the oDSG, a right of rectification only occurred following

---

317 Art. 19 para. 1 item d oDSG.

318 Lukas Bühlmann and Hatun Metin, 'Totalrevision des Schweizer Datenschutzgesetzes vor dem Hintergrund der DS-GVO' (2019) 9(8) Zeitschrift für Datenschutz 356, 359.

319 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7077.

320 See on the constitutional definition of "privacy", *infra* C.III.4.a.

321 This changes under the nDSG as can be seen later in this chapter.

322 "dem normalen Lauf der Dinge entsprechendes Vergessen", *cf.* 109 II 353, [1983] (BGE).

323 122 III 449, [1996] (BGE).

324 Art. 30 et seq. nDSG.

325 Christian Peter, 'Das Begehren um Löschung von Patientendaten' [2019] Jusletter, 9.

326 Art. 30 para. 2 item b nDSG.

327 Art. 31 nDSG.

328 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 17 et seq.

329 Griesinger (n 86), 45; See in more detail on some of such duties *supra* C.III.1.b.

330 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7077.

an unlawful violation of personality, namely a violation of the principle of data correctness, *cf.* Art. 12 para. 2 item a oDSG[331]. However, this violation of personality can always be justified under Art. 13 oDSG[332], for example via prevailing interest if the effort for rectification is disproportionate.

The nDSG now does not connect the right of rectification to the principle of data correctness but explicitly places it behind the regulations for a personality violation. Thus, rectification cannot be denied based on Art. 31 nDSG but only on the reasons listed in Art. 32 para. 1 nDSG, namely prohibition by law (item a) or archive purposes in public interest (item b); an exception because of prevailing (private) interest is nowhere to be found. Ultimately, this leads to the somewhat inconsistent conclusion that incorrect data can be processed if justified by – for example – legitimate interest,[333] but in the same instance must be deleted if demanded by the data subject, because the data is incorrect.[334] This may lead to absurd situations, where the deletion of data is more efficient than the rectification or rectification is plainly disproportionate to deletion and nonetheless requested by the data subject: The controller would be obliged to rectify the data nonetheless. This problem could be solved in practice by interpreting "(in)correctness" restrictively or by granting the controller a right to refusal of rectification due to an abuse of law.[335]

Another new possibility for revocation arises from the new wording of Art. 6 para. 5 nDSG (principle of data correctness) which is not *per se* a data subject right, but states that the controller must take measures to **delete wrong or incomplete data** in context to its purpose. They then must, in principle,[336] act on their own, with action by the data subject not required.[337] This is also true for data processing, which is not necessary for its purpose anymore, Art. 6 para. 4 nDSG (principle of data minimalization). The latter can be transposed into practice via giving reasonable retention periods that must be respected unless a longer period is prescribed by law.[338] However, this period is shorter, if the purpose factually does not exist anymore, for example when a customer cancels his contract, thus giving the data subject some *de facto* controlling powers over the scope of processing.

The question of whether data is **wrong or incomplete** according to Art. 6 para. 5 nDSG[339] cannot be answered uniformly, but is **dependent on the scope and purpose** of processing, the nature of processed data, and the risk of privacy or fundamental rights violation in the individual case.[340] This regulation was implemented

331 Art. 30 para. 2 item a nDSG.

332 Art. 31 nDSG.

333 An example would be, that the correct data does not inflict a harsh privacy infringement upon the data subject (which is likely), but to correct the data on all systems would cause disproportionate costs, *cf.* Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 52. The argument of disproportionate costs, however, cannot be brought up easily. If data is incorrect, this is often due to the controller not having fulfilled his privacy by default obligation under Art. 7 para. 1 nDSG (*infra* C.IV.2.a) and therefore can be held liable to a larger extent, *cf.* Rosenthal, 'Das neue Datenschutzgesetz' (n 37), 50.

334 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 52 et seq.

335 ibid 53.

336 This is in practice enforceable via a claim under Art. 28 ZGB, if the controller does not take action: If the data remains wrong or incomplete, the principle of data correctness is violated, constituting an unlawful violation of personality and opening for the possibility of civil remedies.

337 Bühlmann and Schüepp (n 103), 16.

338 Bieri and Powell (n 86), 4; Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7026.

339 Considerations from the oDSG can be transferred here, whose Art. 5 para. 1 has similar wording, only without a further specification on appropriate measures.

340 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7026.

according to Art. 5 of Convention 108+[341] and must therefore be interpreted in this context. The data must especially be relevant to the purpose, factually correct and, if necessary, updated to the latest state. This leads to a restrictive interpretation of incorrectness and is therefore suitable to restrict a right to rectification in a reasonable extent: For example, if one's surname changes, one can request rectification of the now incorrect name as saved and used by the controller. At the same time, the name becomes factually incorrect in all relevant backups. However, in its purpose to enable the possibility to restore lost data, the correct surname is irrelevant and would therefore not be incorrect under the meaning of Art. 6 para. 5 nDSG.[342]

As a "Swiss Finish", the right to insert a **note of objection**[343] if the correctness cannot be proven remained unchanged in Art. 32 para. 4 nDSG[344].

Art. 28 nDSG contains a **right to "data access or transfer"**, which, different to the right under Art. 25 nDSG, allows the data subject to obtain "raw" personal data disclosed *to* the controller.[345] The right applies to controllers processing the data in an automated manner and where the data is processed by consent of the data subject or in connection to a contract with the data subject.[346]

According to the right to "data transfer" in Art. 28 para. 2 nDSG, internationally often named "**data portability**", the personal data must be transferred to another controller on request, however, under the caveat of such transfer not requiring disproportionate effort. Art. 29 allows the controller to refuse to comply with the request of the data subject on the same grounds as in Article 26 paras 1 and 2, which list grounds for refusal of compliance concerning the right to information.[347]

d. Procedural Aspects

Costs for and effectivity of the rights of the affected persons; consumer accessibility.

Art. 8 para. 5 oDSG prescribes **modalities** for an invoked right to information: As a general rule, the information must be given in written form, as a print or as a photocopy. Specification on this can be found in Art. 1 and 12 oVDSG. If access is denied, the controller of the data file must give reason for their denial, restriction or postponement, Art. 9 para. 5 oDSG[348].

The information covered under Art. 19 nDSG must be given immediately after collecting the data. If the controller collects the data indirectly, the information must be given within a month, Art. 19 para. 5 nDSG. In the nDSG, the data subject's right to information must generally be provided **free of charge** and within 30 days, Art. 25 paras 6 and 7 nDSG (strangely enough, Art. 25 – in differentiation to Art. 19 – speaks of 30 days instead of a month). Nearly identical to the old law, Art. 20 – 23 E-VDSG hold specifications for modalities of the right to information. This is also true for the right to

---

[341] See on the Swiss efforts to ratify convention 108+ *supra* A.I and B.III.

[342] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 53.

[343] Translated from German, "Bestreitungsvermerk". This instrument allows for a compromise, that in case of *non liquet* situations, the principle of *in dubio pro reo* does not fully perish the data subject's doubt.

[344] Art. 15 para. 3 oDSG.

[345] This is markedly different to all personal data "about the data subject" held by the controller, as, in this case, data created by the controller, so-called "synthetic personal data" as in analyses about the individual are not part of the scope of this right, which significantly limits its scope when compared to other international variants of the right.

[346] This potentially restricts the scope of the right to data access or transfer in a substantial manner, as consent is not a central requirement in the Swiss data protection regime, which rather relies on an opt-out approach, *cf.* Art. 12 para. 2 item b oDSG and Art. 30 para. 2 item b nDSG.

[347] See *supra* Section C III 3 a.

[348] Art. 26 para. 4 in slightly different wording.

data access and data transfer as of Art. 28 para. 3 nDSG which refers to the access or transfer to be free of charge, giving the Federal Council regulatory power to specify on this. However, Art. 24 E-VDSG specifies not only on the costs of transfer[349] but on several modalities of Art. 28 nDSG as a whole, indicating that the opening clause in Art. 28 para. 3 refers not only to para. 3 but to all paragraphs of Art. 28, yet again questioning the legal basis for the extensive rulings of the E-VDSG.[350]

4. Enforcement

a. Damages and Compensation

Material and immaterial damages; reparations; profit forfeiture; punitive damages.

Art. 15 para. 1 oDSG does not contain a basis for liability but refers to Art. 28 et seqq. ZGB, which again only allows for the possibility of a **claim for damages** and needs a corresponding basis for liability. Bases for liability are scattered around Swiss private law with the most important (on the area of privacy protection) being Art. 41 and 55 OR and Art. 55 ZGB.[351] Beside this, the Swiss law knows some sectoral claim for damages, *e.g.* in labour law, Art. 328, 328b or in conjunction with Art. 41, 49 OR.[352] Therefore, claims for damages after a breach of data protection law must conform with the general rules for violations of personality under Swiss private law.

Non-monetary compensation can be achieved via the **right of reply** against representation of events in periodically appearing media in Art. 28g et seqq. ZGB. Everyone whose privacy is directly affected by the representation is entitled to this right, *e.g.* allegations that an atheist is in fact a catholic[353], that a marriage is broken[354] or that someone participates in prostitution[355].[356] Therefore, a person's privacy is "affected" whenever the representation makes the claimant appear in an unfavourable public image.[357]

When it comes to **monetary compensation** – para. 1 and 2 only regulate restitution – Art. 28a para. 3 ZGB refers to tort law, regulated in the OR. Here, Art. 41 is relevant for material damages, while Art. 49 is relevant for immaterial damages.[358]

Art. 41 OR can be broken down to having five prerequisites: Unlawful violation of personality (1), infliction of damage (2), adequate causality (3), fault (4) and the scope of liability (5).[359]

The violation of processing requirements under the DSG already constitutes a relevant violation of personality under Art. 28 ZGB (which served as a role model for the DSG) as can be seen in Art. 12 et seq.[360] and 15

---

349 The data subject can only be charged with up to 300 Swiss francs, Art. 24, 23 para. 2 E-VDSG.

350 This is also applicable for the right to information under Art. 25 nDSG, Wermelinger, 'E-VDSG' (n 6) 13 et seq.

351 Thomas Geiser, *Die Persönlichkeitsverletzung insbesondere durch Kunstwerke* (Basler Studien zur Rechtswissenschaft Reihe A vol 21, Helbing & Lichtenhahn 1990) 214 et seqq.

352 4A_518/2020, [2020] (BGer) E.4.2.5.

353 The right to informational self-determination is infringed.

354 The right to protection of private life is infringed.

355 The right to protection of honour is infringed.

356 Matthias Schwaibold, 'Art. 28g' in Thomas Geiser and Christiana Fountoulakis (eds), *Zivilgesetzbuch I: Art. 1 - 456 ZGB* (Basler Kommentar vol 1, 6th edn. Helbing & Lichtenhahn 2018) 325.

357 114 II 388, [1987] (BGE) E.2.

358 Andreas Meili, 'Art. 28a' in Thomas Geiser and Christiana Fountoulakis (eds), *Zivilgesetzbuch I: Art. 1 - 456 ZGB* (Basler Kommentar vol 1, 6th edn. Helbing & Lichtenhahn 2018) 312.

359 Geiser (n 351) 209 et seqq.

360 Art. 30 et seq. nDSG.

para. 1[361] oDSG.[362] However, privacy as protected by Art. 28 ZGB does not exhaust itself in data protection. Instead, it gives a remedy to protect all aspects of privacy as provided by Art. 13 BV, which only in its para. 2 covers data protection. In the first place, there is no uniform definition of privacy. Rather, the constitution protects privacy as a whole – not its individual aspects – which is why Art. 28 para. 1 ZGB contains a general clause ("whoever is being unlawfully violated in their personality"). However, legal scholars and courts have formed some overlapping **categories of personality rights**. At this point, one must acknowledge that these categories are non-exhaustive and should only give judges orientation for the sake of legal clarity. Art. 28 ZGB can apply in cases where these categories were not affected – or *vice versa* cannot apply where categories are affected. This is because Art. 28 ZGB looks to protect personality as a fundamental freedom and does not constitute personality as bundle of subjective rights.[363]

The scope of protection can broadly be divided in three sections: physical area (including right to physical and sexual integrity, life, and freedom of movement); psychological area (including right to maintain relation to related persons and their respect and "integrity of soul") and social area (including right to the own name[364], image[365], voice and word[366] as well as informational self-determination[367], honour and protection of one's private and personal life divided into the public, private and intimate/secret sphere[368]).[369] In terms of data protection, the latter section is most important.

Of course, the right to be forgotten[370] and the right to data protection are also part of the privacy protected by Art. 28 ZGB. Art. 15 oDSG is more specific in this respect, so that a breach of DSG provisions can only be addressed with reference to Art. 15 oDSG, never via Art. 28 ZGB alone.

All these privacy aspects have in common that an infringement would reduce or alter the reputation in professional and/or societal contexts. In order for Art. 28 para. 1 ZGB to trigger, this infringement must pass a certain threshold of intensity in this respect.[371]

However, even if a violation of such privacy is given, monetary compensation is only rarely granted under Art. 28 ZGB in practice. This is because material damages from the infringement of an immaterial good such as privacy can only arise from indirect consequences.[372] These, in turn, do rarely have provable[373] **adequate causality**.[374]

A much more promising approach to compensation is the claim for **immaterial damages** under Art. 28a para. 3 ZGB in

---

[361] Art. 32 para. 2 nDSG.

[362] Vaguely Andreas Meili, 'Art. 28' in Thomas Geiser and Christiana Fountoulakis (eds), *Zivilgesetzbuch I: Art. 1 - 456 ZGB* (Basler Kommentar vol 1, 6th edn. Helbing & Lichtenhahn 2018) 288; the violation can only be remedied under Art. 28 ZGB in conjunction with Art. 15 DSG.

[363] See on this differentiation already *supra* C.I.

[364] 80 II 136, [1954] (BGE); 90 II 461, [1964] (BGE). See also Art. 29 ZGB.

[365] *Minelli* 127 III 481, [2001] (BGE); (n 322); 126 III 305, [2000] (BGE).

[366] Meili, 'Art. 28' (n 362)

[367] See on informational self-determination *supra* C.II.1.

[368] 97 II 97, [1971] (BGE); Geiser (n 351) 51 et seqq.; Meili, 'Art. 28' (n 362) 293.

[369] Meili, 'Art. 28' (n 362) 290.

[370] See on the right to be forgotten already *supra* C.III.3.c.

[371] Meili, 'Art. 28' (n 362) 298.

[372] Geiser (n 351) 211.

[373] The claimant carries the burden of proof for causality according to Art. 8 ZGB, see also Meili, 'Art. 28' (n 362) 306.

[374] An example of adequate causality would be the unlawful public disclosure of sensible data that ultimately leads to the release of the data subject, *c.f.* 5C.57/2004, [2004] (BGer).

conjunction with Art. 49 OR, which allows for **"satisfaction"**[375].

Satisfaction requires an "immaterial injustice"[376], which is objectively a violation of personality and subjectively regarded as a reduction of mental well-being. These prerequisites are cumulative.[377]

Art. 49 OR requires in divergence to Art. 41 "justification by the seriousness of the infringement", which can be understood as an impairment that, due to its intensity, exceeds the measure of what a person must endure according to the currently applicable view of what a person has to tolerate without special legal protection.[378] This becomes especially relevant in data protection contexts in cases of infringements of the secret sphere.[379]

The claim for satisfaction is – according to Art. 49 OR[380] – only subsidiary. Consequently, satisfaction in money will not be awarded if the injuring party was already criminally convicted, rehabilitated the claimant by own means (*e.g.* apology in case of violated honour) or the claimant was able to successfully fight off the infringement by himself (*e.g.* via press release).[381]

Even if monetary satisfaction is granted, it has the only purpose to balance inflicted moral damages[382] and thus, such claims rarely exceed the sum of 10.000 Swiss francs.[383]

Lastly, there exists a possibility to sue for **profit forfeiture** (which is explicitly mentioned in Art. 28a para. 3 ZGB) besides claiming damages.[384]

b. Procedural Aspects

"Threshold" for accessibility; right to initiation; burden of proof; dispute value; "small claims"; alternative dispute resolution; rights to bring/press charges; „rational apathy".

Art. 25 para. 4 oDSG states that disputes vis-à-vis federal bodies (especially the EDÖB, Art. 33 oDSG) work via administrative procedure (based on the Administrative Procedure Act (VwVG)). Procedures with the litigation issue of a violation of privacy are dealt with according to Art. 28, 28a, 28g – 28l ZGB, *cf.* Art. 15 para. 1 oDSG. These claims are civil ones, which is why the Swiss Civil Procedure Act (ZPO) is applicable here in accordance with Art. 1 item a ZPO.[385]

The ZPO knows four main types of action: The action for performance (Art. 84 ZPO), the action to modify a legal relationship (Art. 87 ZPO), the action for a declaratory judgement (Art. 88 ZPO) and the group action (Art. 89 ZPO).

Art. 15 para. 1 oDSG[386] (specifically) and Art. 28a ZGB (generally) name possibilities to take action on an only substantive level.[387] In detail, the claim for prohibiting a threatened infringement (Art. 28a para. 1 no. 1 ZGB), the claim for abatement or removal of existing infringements (para. 1 no. 2), the claim for publication of infringements (para. 2) and the

375 Translated from German, „Genugtuung".

376 Translated from German, „immaterielles Unbill"; *cf.* Schweizerischer Bundesrat, 'Botschaft über die Änderung des Schweizerischen Zivilgesetzbuches: Persönlichkeitsschutz: Art. 28 ZGB und 49 OR' (1982) 133(28) Bundesblatt 636, 680 et seq.

377 Geiser (n 351) 220 with further proof.

378 Schweizerischer Bundesrat, 'Botschaft zu Art. 28 ZGB' (n 376) 681.

379 130 III 28, [2003] (BGE) E.4.2.

380 „No other amends have been made".

381 Roland Brehm, *Berner Kommentar: Kommentar zum schweizerischen Privatrecht; Schweizerisches Zivilgesetzbuch* (5. Auflage, Stämpfli 2021) 645.

382 Meili, 'Art. 28a' (n 358) 312; Brehm (n 381) 648; Geiser (n 351) 219.

383 Brehm (n 381) 675 et seq.

384 133 III 153, [2006] (BGE).

385 Amédéo Wermelinger, 'Art. 15' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 196.

386 Art. 32 para. 1 nDSG.

387 Meili, 'Art. 28a' (n 358) 308.

claim for damages (para. 3) are enforceable via an action for performance; the claim to make a declaration that an infringement is unlawful is enforceable via the action for a declaratory judgement.

Art 59 para. 2 ZPO lists (non-exhaustively) the procedural requirements for all actions to be filed.

Because procedures with data protection as subject matter rarely exceed the dispute value of 30.000 Swiss francs, most data protection disputes are held via **simplified proceedings** (Art. 243 et seqq. ZPO). If the data protection violation threatens to cause not easily reparable harm (Art. 261 para. 1 ZPO), interim measures (Art. 261 et seqq. ZPO) via summary proceedings may be pursued.

The Swiss civil procedure system provides for a mandatory[388] **alternate dispute resolution** before all simplified or ordinary proceedings: the conciliation proceedings, *cf.* Art. 197 ZPO.

The conciliation proceedings are held before special authorities traditionally named "judges of peace"[389] who are independent of the respective court and not rarely laypersons.[390] They shall ensure an oral debate considering even external aspects with the overall goal to reach an agreement making court proceedings irrelevant.[391] However, the authority remains neutral and should neither urge the parties for a settlement nor give authorization to proceed with undue haste.[392]

Legal protection against acts of federal authorities, especially the EDÖB, can be achieved via **appeal** (Art. 44 et seqq. VwVG in conjunction with the Federal Act on the Federal Administrative Court (VGG)) to the Federal Administrative Court, *cf.* Art. 25 para. 4, 33 oDSG,[393] which has the following preconditions:

(a) Subject to an appeal are all rulings as of Art. 5 VwVG, *cf.* Art. 44 VwVG. If the relevant subject is a real act (as it is in cases of Art. 25 oDSG[394]), the appellant must first request a ruling on this real act, *cf.* Art. 25a VwVG.
(b) Anyone has the right to appeal, if they have participated or have been refused opportunity to participate in proceedings before the lower instance[395] (formally affected), have been specifically (materially) affected by the contested ruling and have an interest that is worthy of protection, *cf.* Art. 48 VwVG.
(c) Form and period are regulated in Art. 50 and 52 VwVG. Especially, an appeal can be made at any times if the requested ruling was refused or delayed in issuing.

The Swiss law (neither procedural nor substantial) does not know collective remedies. The legislator explicitly refrained from implementing rules on collective remedies in the nDSG.[396] However, a legislative initiative is currently being considered to facilitate collective enforcement in Switzerland.[397]

---

388 There even is the possibility of penalization of default in Art. 128 ZPO, *cf.* 141 III 265, [2015] (BGE) E.5.

389 Translated from German, „Friedensrichter".

390 Christoph Leuenberger and Beatrice Uffer-Tobler, *Schweizerisches Zivilprozessrecht* (2nd edn, Stämpfli 2016) 324.

391 Schweizerischer Bundesrat, 'Botschaft zur Schweizerischen Zivilprozessordnung (ZPO)' (2006) 157(37) Bundesblatt, 7330.

392 ibid.

393 Art. 41 para. 6 and 52 para. 1 nDSG.

394 Art. 41 nDSG.

395 The Swiss administrative procedural law looks to settle disputes by firstly requiring a complaint to an administrative supervisory instance. However, the EDÖB is such lower instance as under Art. 33 VGG and therefore, a direct appeal to the Federal Administrative Court is possible in this respect.

396 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 6984.

397 Motion 13.3931.

IV. Objective Legal Obligations of the Recipient

1. Duties Concerning Received Data

a. Dependence on Authorization

Of business models, processing variants, terms and conditions.

The DSG, neither old nor new, does not rely on authorization of certain acts of processing from public bodies. However, Art. 11 para. 2 oDSG opens the possibility for state-approved **certification** procedures and quality labels by means of ordinance.[398] The Federal Council acted upon this legal basis for certification in the Accreditation and Designation Ordinance (AkkBV) and the Ordinance on Data Protection Certification (VDSZ), which will be adjusted technologically to the new legal framework.[399] These ordinances regulate the certification of data privacy management systems and products designed to process personal data according to technical ISO standards (Art. 4 et seq. VDSZ). However, this certification system is non-mandatory, and non-compliance only leads to revocation of certification. In Swiss practice, certification is widely regarded as **not practical** from a legal, financial, and technical point of view, which is why the EDÖB has suspended its efforts to establish a comprehensive certification system.[400]

This was largely copied into Art. 13 nDSG, but now adds the certification of services which is regarded as more useful than the certification of products by representatives of economy and politics.[401] If this leads to an utilisation of certification systems in practice, remains to be seen.

b. Notification Duties

Of business models and business activity; of processing activity.

Art. 6 para. 3 oDSG contains, in the context of different modes of cross-border data transfers, **obligations to notify** the EDÖB of guarantees or rules.[402]

Art. 11a para. 3 oDSG (para. 2 for federal bodies) contains the obligation to notify the EDÖB of data files that either regularly processes sensitive data or personality profiles or regularly discloses data to third parties so that the EDÖB may publish a register of data files.[403]

This exists in a similar manner in the new law, though only for federal bodies, in Art. 12 para. 4 nDSG.[404]

A general obligation for **breach notifications** does not exist under the oDSG. Only a manageable number of companies who are specially regulated under the financial market law and therefore subordinate to the FINMA[405] are obliged to report data breaches, *cf.* Art. 29 para. 2 of the Financial Market Supervision Act (*Finanzmarktaufsichtsgesetz* (abbreviated FINMAG)).[406]

Art. 23 nDSG, in paras. 1 to 3, contains an obligation to **consult** with (thus also notify) the EDÖB where the impact assessment according to Art. 22 nDSG[407] resulted in the

---

398 For more detail on self-regulation, see *infra*, C.IV.2.b.

399 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7109.

400 EDÖB, 'Stand der Produkt- und Dienstleistungszertifizierung' (19 May 2022) <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung/stand-der-produkt--und-dienstleistungszertifizierung.html> accessed 19 May 2022.

401 ibid.

402 This notification duty was abandoned in the nDSG, *cf.* Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 29.

403 See on these (rarely used) register *infra* C.IV.1.c.

404 See on records of processing activities *infra* C.IV.1.c.

405 Federal Financial Market Supervisory Authority.

406 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 62.

407 See on data protection impact assessments *infra* C.IV.2.a.

assessment that processing activity is of high risk for the data subject. However, such a consultation with the EDÖB is not necessary when the controller has consulted its data protection advisor.[408]

Art. 24 nDSG contains provisions for what is internationally called a data breach or data leakage notification duty: Para. 1 requires the controller to notify the EDÖB "as quickly as possible of a breach of data security presumably leading to a high risk[409] to the personality or fundamental rights of the data subject". In this context, one should note that "breach of data security" is legally defined in Art. 5 item h nDSG.[410] Art. 24 para. 2 nDSG then states the necessary contents of such notification, being the type of violation of data security, its consequences and countermeasures taken. Para. 3 requires that also the processor must notify the controller of breaches (but only the ones presumably leading to a high risk) as quickly as possible, which usually translates to a time frame of 24 to 72 hours.[411]

Para. 4 contains the (rather vague) obligation of the controller to inform the data subject "where necessary for their protection or where the EDÖB requires it" – it should be noted here that the EDÖB can only require action of which it is aware, thus likely only to be effective where notifications have already occurred under para. 1. Para. 5 then contains reasons where notification of the data subject may be restricted, postponed, or deferred.

It is difficult to assess how effective this notification requirement will be: Due to the restriction of the notification under para. 1 to cases of high risk and with such an assessment, due to the nature of knowledge of such violations of data security, in the hand of the controller, this requirement may be very rarely acted upon in practice. Additionally, a violation of Art. 24 nDSG is not connected to criminal sanctions[412] and beyond this cannot stipulate a privacy infringement under Art. 30 nDSG. Nonetheless, the restriction of use of such notifications in criminal proceedings for the controller under Art. 24 para. 6 nDSG may incentivise the controller to notify the EDÖB more often. It remains to be seen how effective this instrument will prove in practice.

Due to this notification duty and the accompanying documentation duties in Art. 12 nDSG[413], a *de facto* obligation to run a **data privacy management system**[414] is inflicted upon the controller.[415]

c. Documentation

Accountability.

The oDSG requires the EDÖB in its Art. 11a to hold a **register of data files** that shall be publicly accessible via internet.[416] It contains all data files of public organs (para. 2) and all private data files regularly processing

[408] See on the data protection advisor *infra* C.IV.2.a.

[409] The controller must assess a high risk for every individual case, considering the probability of a breach and more importantly the intensity of the threatened privacy infringement. This term must be delimited from high-risk profiling (*supra* C.II.1.) and high risk under Art. 22 nDSG (*infra* C.2.a). See on this Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 60 et seq.

[410] See *supra* C II.1.

[411] Griesinger (n 86), 26.

[412] The notification can only be forced via Art. 51 para. 3 item f nDSG without further sanctions. However, future wilful disregard of such orders may be criminalised under Art. 63 nDSG.

[413] See following section.

[414] Translated from German, "Datenschutzmanagementsystem".

[415] Ursula Sury, 'Das neue Datenschutzgesetz der Schweiz im Vergleich zur DSGVO' (2021) 44(3) Informatik Spektrum 221, 222 <https://dl.gi.de/handle/20.500.12116/36519>.

[416] EDÖB, 'Datareg 3.2 - WebDatareg' (21 April 2022) <https://www.datareg.admin.ch/> accessed 21 April 2022.

sensitive data or personality profiles or regularly disclosing data to third parties (para. 3) with corresponding notification duties. However, the register is rarely used in practice[417] and thus was abandoned under the nDSG.[418]

In Art. 12, the nDSG provides for a much more comprehensive requirement concerning documentation: In para. 1, it states that the controllers and processors must keep **records on their processing activities**. This record shall be an "internal counterpart" to the external privacy statement[419] and shall keep track on the basic parameters of one's data processing. It is therefore in its scope largely comparable to the information obligation under Art. 9 nDSG.[420]

Paras. 2 and 3 give more information on what information at least must be kept in the controller's and processor's records, respectively. Para. 4 states that federal bodies must notify the EDÖB of their records – replacing the old obligation of private entities as well as federal bodies. Thus, under the nDSG private persons are not required to notify the EDÖB. Art. 56 nDSG states that it is the responsibility of the EDÖB to keep the register of processing activities of federal bodies, which is to be published.

Art. 12 para. 5 nDSG contains a provision allowing the Federal Council to provide for exceptions for companies with less than 250 employees and whose data processing activities pose only a low risk of violations of personality, which is to be acted upon in Art. 26 E-VDSG, further specifying that companies who do not process sensible data to a large extent or conduct are exempt from high-risk profiling.

Further obligation for documentation, especially a general one comparable to Art. 5 para. 2 GDPR cannot be found in the nDSG despite being discussed in earlier drafts.[421]

d. Processing Requirements

Prohibition subject to permission; balancing of interests; restrictions for terms and conditions; business practices; APIs/interfaces for third parties.

As already put forward,[422] the nDSG does not rely on a prohibition subject to permission for the private sector, but only for the public sector. Rather, data processing is allowed as long as no unlawful violation of personality occurs (**permission with subject to prohibition**). Whilst the threshold to a privacy infringement is not particularly high (Art. 12 oDSG[423]), it can be justified by consent, overriding interest or law (Art. 13 oDSG[424]), thus allowing the processing in general. With this approach, the Swiss system focuses on the **safeguarding of its principles** (Art. 12 para. 2 item a oDSG), an opt-out approach (Art. 12 para. 2 item b oDSG), and a risk-based approach around the disclosure of sensible data to third parties (Art. 12 para. 2 item c oDSG).

As far as Swiss GTCB law is concerned, the so called "**rule of unusualness**"[425] must be acknowledged for data protection purposes. It states that if a general consent of terms and condition is declared, those clauses are

---

417 According to the aforementioned website, the register contains 2.790 files. This might seem a lot on the first sight. It must be considered, however, that the term of data file is interpreted very broadly (see *supra* C.II.1) and includes every digital actor who holds data of more than one person. In the highly digitalized world of today, one can expect a lot more data files under this meaning in a post-industrial country like Switzerland, counting nearly 9 million citizens.

418 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 54.

419 *i.e.* the information obligations, *cf. supra* C.III.2.a.

420 Bieri and Powell (n 86), 12.

421 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7035; Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 53.

422 *Cf. supra* C.I.

423 Art. 30 nDSG.

424 Art. 31 nDSG.

425 Translated from German, "Ungewöhnlichkeitsregel".

exempt from consent which are unusual to the context (*i.e.* surprising or alien to usual business practices) and not specifically called to attention.[426] This becomes relevant whenever one term in the GTCB contains a declaration of consent as required by Art. 13 para. 1 oDSG and the data subject consents to all GTCB without taking special notice of such declaration.[427] This requires that (a) it is sufficiently apparent that by asking for consent to GTCB, the controller also wants consent for data processing (*e.g.* that data will be processed after signing the contract)[428] and (b) the scope of processing is reasonable and to some extent foreseeable for the data subject (*i.e.* a type of processing is unusual if the data subject has no reason to expect it).[429]

2. Monitoring

a. Recipient Self-Monitoring

Self-restrictions; compliance mechanisms; internal responsibilities (company privacy officers; ombudspersons).

Art. 7 nDSG - a partial innovation compared to the oDSG - is headed "Data Protection by Technology and Data Protection by Privacy-Friendly Default Setting"[430]. It creates in paras. 1 and 2 broad obligations for the controller to technologically and organizationally structure processing of personal data in a manner allowing for compliance with data protection provisions, especially the principles in Art. 6 nDSG,[431] starting with the planning phase, and (para. 2) to use such measures in a manner "proportionate to the state of technology, type and scale of processing, and risk for personality and fundamental rights of the data subject". Para. 3 requires the controller to use the settings as default that – if several options are possible for the data subject – are least infringing for the data subject's privacy.[432] The data subject can always opt out from this by agreeing to the controller's offer to change the pre-settings.[433] This can be understood as a "**privacy by design**" and "**privacy by default**" approach as can be found in the GDPR[434].[435] The latter was nowhere to be found in the oDSG, while the "privacy by design" approach – even if not explicitly mentioned – can be seen in Art. 7 oDSG, the (broader) obligation to guarantee data security: "adequate technical and organizational measures" under the meaning of Art. 7 para. 1 oDSG includes measures to prevent data security breaches in time, *i.e.* in the planning phase.[436]

An interesting difference between the old and the new approach is that in the nDSG "privacy by design" is no principle of data processing anymore.[437] Thus, a violation of it cannot lead to a privacy infringement under Art. 30 para. 1 nDSG[438] and is no longer enforceable by individual actors and can only be enforced by the EDÖB.[439] It remains to be seen in practice to what extent "privacy by

---

426 119 II 443, [1993] (BGE) E.1a; 138 III 411, [2012] (BGE) E.3.1.

427 Whilst the applicability to consent is undisputed, the applicability to information obligations is not, *cf.* Bühlmann and Schüepp (n 103), 22.

428 ibid 30.

429 Vasella, 'Einwilligung im Datenschutzrecht' (n 206) 15.

430 Own translation.

431 See on the principles of Swiss data protection law *supra* C.I.

432 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 22.

433 Rosenthal, 'Entwurf des nDSG' (n 229) 17.

434 Art. 25 GDPR.

435 Sury (n 415), 222.

436 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 21.

437 The in comparison to Art. 7 oDSG narrower Art.8 nDSG does not include an obligation for "privacy by design" measures anymore.

438 This only, if one follows the reasoning that the principle of legality does only include the provisions of the DSG that directly connect to the individual act of processing, see *supra* C.III.1.a.

439 Rosenthal, 'Entwurf des nDSG' (n 229) 19; see on enforcement by the EDÖB *infra* C.IV.3.a.

design" will be read into the principle of data security (Art. 8 para. 1 nDSG) as it is under the oDSG.

Art. 10 nDSG introduces rules for the appointment of a **data protection advisor** (similar to the "Data Protection Officer" in the GDPR, with the main difference that under the nDSG the appointment of the advisor is **not mandatory** but voluntary). Such a data protection advisor is responsible for internal implementation and education on data protection topics and serves as a point of contact to the competent regulatory authorities in the field of data protection. As of Art. 10 para. 4 nDSG, further provisions on such advisors are to be enacted by the Federal Council, which it did in Art. 27 – 30 E-VDSG, which – besides the requirements for qualification most importantly grants the advisor in Art. 29 a right for access to all relevant information to fulfil his duties.

Under the oDSG, the concept of a data protection advisor of the nDSG can only be compared to the data protection officer under Art. 11a para. 5 item e oDSG and Art. 12a et seq. oVDSG. They have – besides easing the effort for data protection compliance – the only purpose that a register under Art. 11a oDSG[440] must not be declared to the EDÖB if the data protection officer supervises it.

Art. 14 and 15 nDSG require foreign private entities who process personal data of individuals in Switzerland to appoint a **representative** when crossing certain thresholds as listed in Art. 14 items a-d. This representative is the point of contact for the EDÖB and data subjects in Switzerland and their contact information must be published by the controller according to Art. 14 para. 3.

Art. 22 nDSG provides for situations where a **data protection impact assessment** must be made by the controller in advance of processing of personal data: This is, as of para. 1, the case where such processing may cause a high risk for the personality[441] or the fundamental rights of the data subject. For multiple similar acts of processing, a common assessment can be made. Para. 2 contains rules for when such high risk is to be assumed and para. 3 states the necessary contents of such an assessment, which is mainly an evaluation of risk to the data subject and the mitigating measures taken.

Para. 4 excludes private entities processing personal data from creating such an assessment where the processing of the data is required by law.

Para. 5 allows private controllers to refrain from creating such a data protection impact assessment when using a product certified under Art. 13 nDSG, when adhering to an industry association rulework[442].[443]

Art. 23 nDSG, in paras. 1 to 3, requires the controller to **consult with the EDÖB** in certain situations where the assessment leads to the conclusion that a high risk remains despite countermeasures taken by the controller.[444] Para. 4 of Art. 23 nDSG allows the controller to refrain from consulting with the EDÖB where they have consulted with the data protection advisor – this being one of the central (if not the only)[445] legal

---

[440] See on this register of data files *supra* C.IV.1.c.

[441] See on the requirements of a "high risk" *supra* C.II.1.

[442] See *infra* C.IV.2.b.

[443] Even though no such certification exists under the oDSG, it remains to be seen if this changes under the nDSG.

[444] It is also highly questionable as to whether this instrument will work in practice, as this would require the controller to take the legal view that their own measures are inadequate, and enforcement of this obligation without the EDÖB obtaining knowledge is unlikely – however, this provision may be effective in practice if the EDÖB is perceived as useful by controllers.

[445] Rosenthal, 'Entwurf des nDSG' (n 229) 63.

compliance benefits of appointing such an advisor.

A comparable institution to the data protection impact assessment under the oDSG can only vaguely be found in the federal bodies' obligation to notify the EDÖB of all projects involving automated processing of personal data under Art. 20 para. 2 oVDSG.

b. Regulated Self-Regulation

Industry associations.

Industry associations may create **codes of conduct** under Art. 11 nDSG, which will be published and reported on by the EDÖB. The only (minimal) requirements for a code of conduct are that it must be at least as strict, more concrete than the nDSG and only be applicable for the area of the association handing in the code of conduct.[446] If these requirements are met, the code may only address a certain aspect such as definitions of "high risk" cases, retention periods or data transfer abroad.

Apart from *de facto* advantages such as easier compliance and a broader basis of trust, submitting to a code of conduct, which adheres to protection of privacy and the individual's fundamental rights, may exempt the controller of performing a data protection impact assessment, *cf.* Art. 22 para. 5 nDSG. A code of conduct does not grant further legal protection despite this being discussed in the early draft.[447]

According to Art. 11 para. 2 nDSG, the EDÖB must publish a statement to every code of conduct drafted under para. 1. As the nDSG has not yet entered into force and such codes of conducts being a novelty, the EDÖB has thus not published any such codes of conduct yet.

The oDSG does not know such form of self-regulation apart from certification under Art. 11 oDSG.[448]

Additionally, the EDÖB is obligated to publish non-binding "**best practices**" under Art. 58 para. 1 item g nDSG. He must especially consider interests of industry associations, which can therefore give recommendations for best practices.[449] Even though the obligation to "involve interested groups"[450] has not made it into the final version of the nDSG, the aforementioned requirement for participation of industry associations could *de facto* be read into Art. 58 para. 1 item g nDSG ("(…) considers the peculiarities of the respective area (…)").

c. Supervisory Authorities

Data protection authorities; competition authorities; economic oversight authorities.

Art. 26 oDSG[451] establishes the office of the Federal Data Protection and Information Commissioner (*Eidgenössicherscher Datenschutz- und Öffentlichkeitsbeauftragter,* abbreviated **EDÖB)**, who is appointed for four years and can be re-elected up to two times.

Art. 27 – 32 oDSG enumerate the responsibilities (and powers) of the EDÖB. These being: Supervision of data protection compliance by federal bodies with exception of the Federal Council (Art. 27); consulting of private actors (Art. 28) and reporting to the National Assembly (Art. 30). Art. 31 contains further responsibilities concerning supervision of the oDSG regulation in practice.

The nDSG, in Art. 4, at the beginning of the law, rather than at the end in a special section,

---

[446] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 65.

[447] ibid.

[448] See on certification *supra* C.IV.1.a.

[449] Eidgenössisches Bundesamt für Justiz, 'Vorentwurf nDSG' (n 5) 20.

[450] Art. 8 para. 2 of the early draft of the nDSG.

[451] Art. 43 nDSG.

names in overly broad and unspecific wording the function of the EDÖB in para. 1: "The EDÖB supervises the application of federal data protection provisions". Para. 2 of the same article contains an enumeration of federal bodies not under supervision of the EDÖB, being the National Assembly, the Federal Council, the federal courts, the federal prosecutor, and federal executive organs in connection to processing of personal data related to judicial activity or international legal assistance procedures.

Further details on the EDÖB are contained in Articles 43 to 59 nDSG, dealing with further responsibilities, powers, and internal organisation.

The responsibilities of the EDÖB are slightly extended in the nDSG.[452] The most important changes are found in Art. 49, 52 and 54 et seq. nDSG. Art. 49 para. 1 nDSG stipulates that the EDÖB must investigate violations of data protection regulation *ex officio*. Also, the EDÖB does not work with (not binding) **recommendations** anymore as under the oDSG[453] but with (binding) **rulings** as under the VwVG, *cf.* Art. 52 para. 1 nDSG.

Further, Art. 54 and 55 contain more detailed regulation concerning administrative assistance (abroad).

d. (Specific) Criminal Prosecution

Specific prosecutors for informational crimes; (situational/special) investigators.

In the absence of special provisions concerning the few criminal offences in the oDSG, the competent prosecution authority according to the general provisions of Art. 12 and 22 of the Criminal Procedure Code (*Strafprozessordnung,* abbreviated StPO) can be assumed, *i.e.* the cantonal police, the public prosecutor, and the authorities responsible for prosecuting contraventions. This will be only clarified in Art. 65 para. 1 nDSG. A special criminal prosecution authority addressing only data protection does not exist.

Nonetheless, the EDÖB can **file a complaint** or exercise the rights of a **private claimant** (Art. 108 et seqq. StPO) according to Art. 65 para. 2 nDSG. Thus, he can bring his special investigative powers[454] to trial. A pendant to this cannot be seen in the oDSG, however, the EDÖB can utilise his (rather limited) investigative powers under the oDSG by filing a complaint before the criminal court, whereto he is entitled even without Art. 65 para. 2 nDSG under Art. 301 StPO entitling everyone to file a complaint.

Some federal agencies and cantonal police departments certified by the Swiss Federal Office of Communication have founded special units investigating and prosecuting **cybercrime** under Swiss domains on the internet.[455] Art. 15 para. 1 item a of the Ordinance on Internet Domains (*Verordnung über Internet-Domains,* abbreviated VID) expressly establishes the protection of sensible data against illegal methods as a responsibility of these authorities besides the protection against malicious software, which allows for the interpretation that said certified authorities do not specialise on "simple" data protection but rather on protection against fraudulent behaviour on the internet.

e. Procedural Aspects

Investigation powers; equipment of controlling institutions.

Art. 29 oDSG deals with the modalities of **investigation by the EDÖB** of private

---

[452] See on the large extension of powers *infra* C.IV.3.a.

[453] *Cf.* Art. 29 para. 3 oDSG.

[454] See *infra* C.IV.2.e.

[455] A list of these authorities can be found at Bundesamt f K BAKOM, 'Bekämpfung der Internetkriminalität' (29 April 2022) <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html> accessed 29 April 2022.

parties, the (obligation to) supervision of federal bodies being stipulated in Art. 27. However, Art. 29 para. 1 oDSG includes no obligation to act[456] and is further restricted to certain types of violations, namely system errors, cases where data shall be registered under Art. 11a oDSG[457] and where an information obligation under Art. 6 para. 3 oDSG[458] exists. According to Art. 29 para. 2 oDSG, the EDÖB has the powers to request access to files, obtain information and be shown the data processing. By doing so, he creates a *de facto*[459] **duty to cooperate**, the violation of which is punishable by Art. 34 oDSG, but he cannot enforce his powers by his own.[460]

If the investigation leads to a **recommendation** that the controller shall change or cease his data processing practices (Art. 29 para. 3), this is also only enforceable via turning to the administrative court (para. 4).

Art. 49 to 55 nDSG deal with the procedure of investigation of data protection violations by the EDÖB for both, private and public actors. Art. 49 para. 1 nDSG requires the EDÖB to investigate federal bodies or private persons by itself or upon being made aware by third parties. The EDÖB is now *ex officio* obligated to hold investigations if he has reason to assume a violation of data protection regulation. Because this could overwhelm the EDÖB with formal procedures, he is allowed to refrain from investigations of minor significance according to Art. 49 para. 2 nDSG and can keep on giving recommendations where he deems them sufficient as well as issue a warning where the controller has taken measures belatedly (Art. 51 para. 5).[461]

The EDÖB may request the information necessary to perform an investigation under Art. 49 para. 1, *cf.* para. 3. A direct duty to cooperate follows from this, which can be enforced by **coercive measures** listed in Art. 50 nDSG.[462] These include orders to obtain access to documents and areas as well as to examine witnesses and obtain expert opinions, as well as allowing the EDÖB to ask for the assistance of other federal agencies or of the police. Art. 54 and 55 allow the EDÖB to cooperate with Swiss and international agencies on the area of data protection by means of information exchange.

Art. 59 nDSG allows the EDÖB to collect **fees** from private persons for certain activities – included in this list are mainly provisions dealing with organizational compliance rather than actions affecting data subjects as individuals. The most important actions subject to charge are measures under Art. 51 nDSG[463]. Art. 45 E-VDSG specifies fees amounting to 150 to 300 Swiss francs per working hour. Apart from this, the Swiss General Fee Ordinance applies. If one compares this to Art. 33 oVDSG or even Art. 23 E-VDSG, this amount seems unreasonably high especially for actions of the EDÖB such as consultation following a data protection impact assessment (Art. 23 para. 2 nDSG), which is required by law and can often not be averted by the controller.[464] It therefore remains to be seen, whether this

---

[456] Bruno Baeriswyl, 'Art. 29' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 350.

[457] See on data file registers *supra* C.IV.1.c.

[458] See on data transfer abroad *supra* C.III.2.b.

[459] In contrast to Art. 27 para. 3 oDSG, Art. 29 para. 3 does not speak of cooperation by the private actor. However, it follows from Art. 34 para. 2 item b oDSG that the private actor may neither give wrong information, nor refuse cooperation entirely.

[460] Baeriswyl, 'Art. 29' (n 456) 353.

[461] Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 67.

[462] ibid.

[463] See on these (comprehensive) administrative measures at once.

[464] Wermelinger, 'E-VDSG' (n 6) 14.

fee regulation will make it into the final version of the revised VDSG.

3. Enforcement

a. Intervention Concerning Data Processing

Restriction and prohibition of data processing.

Administrative interventions by the EDÖB are rarely or never seen in the oDSG. Apart from calling to the administrative court to enforce recommendations (Art. 29 para. 4 oDSG), the EDÖB can apply to the president of the first division of the Federal Administrative Court for **interim measures** if the data subjects are threatened with a disadvantage that cannot be easily remedied, *cf.* Art. 33 para. 2 oDSG. These interim measures may for example contain a temporary prohibition of data processing[465] and can even be ordered by court without hearing the counterparty.[466] The procedure is governed by analogy of Art. 79 to 84 of the Federal Act on Federal Civil Procedure (*Bundesgesetz über den Bundeszivilprozess* (abbreviated BZP), *cf.* Art. 33 para. 2 oDSG.

Interventions under civil law are listed in Art. 15 oDSG and can be enforced via individual action.[467]

Art. 51 nDSG as a novelty gives the EDÖB the right to **bindingly order** parties violating data protection provisions to modify, suspend or cease processing of personal data and to delete personal data (para. 1), as well as prohibit disclosure of personal data abroad (para. 2), as well as order federal bodies or private persons to comply with certain obligations (such as information obligations or to conduct a data protection impact assessment) under the nDSG, enumerated in para. 3 and 4. Whilst only para. 1 and 2 directly concern data processing, paras. 3 and 4 shall enforce organisational compliance.[468] All measures are taken via binding ruling as of Art. 5 VwVG. Even if this gives the EDÖB immensely increased administrative powers, he can never order measures that go beyond what the nDSG normally requires, *e.g.* access to information when grounds for refusal exist or a data protection impact assessment when the prerequisites of Art. 22 nDSG are not given.[469] Nonetheless, the EDÖB is granted significantly more freedom and efficiency in practice in his enforcement powers when compared to the prior situation.

Art. 52 para. 1 nDSG specifies the administrative procedure of rulings under Art. 51 nDSG, referring to the VwVG.

b. Intervention Concerning Business Models

Competition and economic authorities; government monopolies.

Addressing **data-based business models** as such is the responsibility of the Competition Commission (*Wettbewerbskommission,* abbreviated WEKO): companies in Switzerland cannot **misuse their market-dominant position** in the data sector in a way that would disadvantage trading partners or competitors, *cf.* Art. 7 (para. 2 item c, so called "exploitative abuse"[470]) of the Cartel Act (*Kartellgesetz,* abbreviated KG).[471] This constellation gained public attention in recent times due to various attempts around the world to regulate Big Data as held by for example Facebook or Google. However, the WEKO refrains from taking any measures

---

465 *Google* (n 81).

466 So called supervisory measure, *cf.* only A-3831/2012, [2012] (BVGer) E.

467 *Supra* C.III.4.b.

468 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7093.

469 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 68.

470 Translated from German, "Ausbeutungsmissbrauch".

471 Natalie Gratwohl and René Höltschi, 'Facebook: Deutsches Bundeskartellamt setzt Grenzen' *Neue Zürcher Zeitung* (7 February 2019) <https://www.nzz.ch/wirtschaft/facebook-deutsches-bundeskartellamt-setzt-grenzen-ld.1458137> accessed 30 May 2022.

against Facebook where a parallel German (or EU) decision on the correlation of antitrust and data protection law[472] was or will be made.[473] It can be assumed that this hesitation is due to the fact that companies doing business within Europe align their business practices cross border, thus – even though only legally necessary in the European Union – it is organisationally easier for companies to refrain from practices illegal under neighbouring (EU) law also in Switzerland.[474] Therefore – even here on a factual level – Swiss legal practice follows a ***de facto* autonomous implementation**:[475] Facebook's adherence to the foreign ruling is expected by Swiss authorities[476] and therefore, compatibility with Swiss law – and simultaneous business model related enforcement – needs not (yet) to be examined. Consequently, the question, whether Swiss antitrust law, which aims to protect effective competition and not consumer rights or data protection laws[477], applies in cases of abusive/excessive collection of data vis a vis the trading partner (and not the competitor),[478] does not need to be answered (also: yet).

In conclusion, Switzerland does not follow other highly digitalised states such as the EU or the USA in regulating data monopolies of big data businesses; the WEKO even explicitly limits itself to observing the development of such big tech players on the digital markets of other countries and to intervening only restrictively in order to protect unknown new opportunities.[479]

This finding somewhat corresponds with the one regarding the Swiss-US Privacy Shield:[480] The WEKO justifies its inaction here with "efficiency",[481] from which it can be concluded that it wants to save capacities and investigative measures that the EU carries out anyway. Even though this is not exactly "**copycat litigation**"[482] (the WEKO does not plan on taking any action against subjects of EU measures), it follows the same reasoning: it would be easier to await reaction to EU litigation than to litigate by oneself.

c. Penalties for Data Processors

Prohibition orders concerning business activities; company sanctions; revenue-based sanctions.

The nDSG (as well as the oDSG) intentionally refrained from enabling the EDÖB to impose **administrative (monetary) sanctions**.[483] To not overload the EDÖB, the administrative expense shall stay with cantonal authorities.[484]

---

472 *Facebook* [2020] KVR 69/19, [2020] 73 Gewerblicher Rechtsschutz und Urheberrecht 1318-1331 (BGH).

473 Wettbewerbskommission (WEKO), 'Jahresbericht 2021' 27.

474 Neither have antitrust rulings in Switzerland on market-dominating data power been issued against Facebook since the BGH judgement in 2020 (n 472), nor has the Competition Commission initiated corresponding investigation proceedings, as per its annual reports for the last three years. See on this assumption also Gratwohl and Höltschi (n 471).

475 See on the autonomous implementation and the high influence of the European Union and its law as well as its legal practices already *supra* A.II.

476 Wettbewerbskommission (WEKO), 'Jahresbericht 2021' (n 473) 27.

477 Note that as of the nDSG, data protection matters are also regarded consumer rights matters, *cf. supra* A.II.

478 Monique Sturny, 'Facebook-Entscheid des Bundeskartellamts zu Nutzerdaten' (30 May 2022) <https://datenrecht.ch/facebook-entscheid-des-bundeskartellamts-zu-nutzerdaten/> accessed 30 May 2022.

479 Wettbewerbskommission (WEKO), 'Jahresbericht 2021' (n 473) 30; see also Wettbewerbskommission (WEKO), 'Jahresbericht 2016' 27 et seq.

480 See on the Swiss-US Privacy Shield *supra* C.III.2.b.

481 Wettbewerbskommission (WEKO), 'Jahresbericht 2021' (n 473) 27.

482 Bradford (n 11) See also *supra* C.III.2.b.

483 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 6944, 7092.

484 Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 66.

The Swiss enforcement system relies heavily on criminal sanctions, which are to be elaborated forthwith. Critics called for greater use of administrative penalties with reference to the GDPR[485] and the possible over-penalisation of employees,[486] but this was not adopted in the final version of the nDSG. It was reasoned that otherwise the fundamental decision under criminal law to require **specific organizational culpability for corporate criminal liability** (Art. 102 StGB) would be strongly relativized by introducing administrative sanctions sweepingly attributing liability to a company.[487] The Federal Council also argues that – with reference to sectors in which administrative sanctions of a punitive nature traditionally exist in Switzerland (*e.g.* postal services, gambling or antitrust law) – this sweeping nature is only justified in the case of large companies, though not in the case of small and medium-sized enterprises which – to a different extent than in the sectors mentioned – are also covered by the scope of application of the nDSG.[488]

d. Penalties for Individual Actors

Directors' liability; individual criminal sanctions.

General criminal offences concerning the infringement of one's privacy are largely stipulated in Art. 179 et seqq. StGB. The range of criminal sanctions differs from mere financial penalties to prison sentences of up to three years, depending on the committed offence. Further, the court may order forfeiture of assets, *cf.* Art. 70 et seqq. StGB.

Most notable in the context of data protection is Art. 179^{novies}, which penalises the unauthorised obtaining of sensible personal data from a data file (this prerequisite is cut after the revision of the DSG) which was not made publicly accessible and the newly introduced Art. 179^{decies} penalising identity theft. Under this norm it is forbidden to use another's identity without their consent to damage that person or to confer an advantage, whereas "identity" is understood broadly and refers to all information that could make a person identifiable.[489] Therefore this new offence is likely to have a wide scope of applicability.

It is also a criminal offence to **disclose secrets** of any kind, which is penalised in Art. 320 et seqq. StGB. A secret is any fact which is known only to a limited circle of persons and in the confidentiality of which the owner of the secret has a justified interest - the will to maintain confidentiality must also have been expressly or implicitly manifested.[490] This (material) concept of secrecy also applies to the regulation of the DSG, especially Art. 35 oDSG[491].[492]

Alongside those general penal provisions, both, the old and the new DSG know special penal provisions in its fifth or rather seventh chapter.

Art. 34 and 35 oDSG penalise giving wrong information despite an obligation, *e.g.* under Art. 8 oDSG; refraining from giving information despite an obligation under Art. 14 oDSG; failing to give notification under Art. 6 para. 3 or Art. 11a oDSG, a violation of a duty to cooperate under Art. 29 or the unauthorized disclosure of sensible data or personality profiles that were necessarily obtained in the course of one's professional practice or as assistant of said person (**professional confidentiality**).

---

485 Enforcement of the GDPR relies largely on administrative sanctions, *cf.* Art. 83, 84 GDPR, which explicitly speak of "sanctions".

486 See on this argument in more detail *infra* C.IV.3.d.

487 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7098 et seq.

488 ibid 7099.

489 ibid 7128.

490 114 IV 46, [1988] (BGE) E.2.

491 Art. 62 nDSG.

492 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7102.

Art. 60 to 63 contain the penal provisions in the specific area of data protection under the nDSG. Art. 60 largely resembles Art. 34 oDSG. Art. 61 nDSG criminalises violations of certain duties of care. These include the disclosure of personal data abroad without compliance with Art. 16 and 17 nDSG, usage of a processor without fulfilling the requirements of Art. 9 nDSG and failing to reach the minimum requirements for data security as stipulated under a ruling of Art. 8 para. 3. Lastly, and important to ensure the authority of the EDÖB, **noncompliance with its rulings** is also penalized in Art. 63.

Most remarkably, the Federal Council decided to greatly extend professional confidentiality in Art. 62 nDSG. It reasoned that in the modern era with its mass distribution of smartphones and the possibility to save and process more and more data calls for a **comprehensive protection of secrecy**.[493] Now, the professional confidentiality shall not only apply for sensible data where knowledge of such data was required for the profession. Rather, it applies for all personal data which a person is aware of in the exercise of his profession which requires such personal data, thus creating sort of a "**professional confidentiality for everybody**" and aligning it to the general professional secrecy in Art. 321 StGB.[494] Some problems in the delimitation between Art. 62 nDSG and Art. 321 StGB may arise from this, which are not new to the DSG.[495] Art. 35 oDSG serves as a fall-back offense for those groups that are not covered by Art. 320 et seq. StGB.[496] This groups are only extended in Art. 62 nDSG but this does not change anything of the character of Art. 62 nDSG as a fall-back.

Overall, the legislator introduced **sharper criminal sanctions** for persons handling personal data in any manner.

Penalties of the DSG are mainly monetary sanctions of up to 250.000 Swiss francs, whereas this penalty was cut by half in comparison to the originally intended 500.000 Swiss francs in Art. 50 of the early draft to the nDSG (*Vernehmlassungsentwurf DSG* (abbreviated VE-DSG (2016)).

The impact of this cut should be marginal, as such sanctions were rarely acted upon in the last 30 years.[497]

It must also be noted that all criminal sanctions under old and new DSG **require wilful action**; Swiss specific data protection law does not include situations of (mere) negligence. Further, all provisions under the oDSG are offences prosecuted only on complaint and have – in general – rather narrow elements and are thus **not often acted upon** in practice by criminal courts.[498] Therefore, even though the nDSG introduces new and sharper criminal data protection offences, they remain – especially because of the element of wilful intent – **narrow and few** in number.

A peculiarity of the Swiss sanction system is **corporate criminal liability** in Art. 102 StGB with the possibility of sanctions of up to five million Swiss francs. However, corporate liability is subsidiary to the liability of a natural person: According to Art. 102 para. 1 StGB, businesses can only be held liable if it is not possible to attribute the

[493] ibid.

[494] *Cf.* The wording "offenbaren" ("to disclose" as in "to reveal") in contrast to Art. 35 oDSG "bekanntgeben" ("to disclose" as in "to announce"), Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 72.

[495] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7102.

[496] Kurt Pärli, 'Art. 35' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 386.

[497] Jens Stark, Interview with David Rosenthal (24 November 2021).

[498] Kurt Pärli, 'Art. 34' in Bruno Baeriswyl and Kurt Pärli (eds), *Datenschutzgesetz (DSG)* (Stämpfli Verlag 2015) 380.

felony to any specific natural person due to the inadequate organisation of the undertaking. Thus, the criminal provisions of the oDSG were criticised for potentially enabling **over-penalisation of employees** that have no decision-making authority.[499] It was especially feared that employees who handle personal data daily must bear the risk of criminal prosecution and – given that there are no administrative sanctions – companies are unjustifiably released from liability.[500]

The Federal Council, however, does not see this danger as most of the criminally relevant behaviours are linked to the controller, who is often a legal entity and whose criminal liability is borne by its representatives according to Art. 29 StGB and Art. 6 VStR.[501] An Employee with no own decision-making authority is very often excluded from this liability, *cf.* Art. 29 item c StGB. The few cases of penalisation in which the liable controller is not the legal entity, but its employee, are tolerable.[502] This somewhat mirrors the risk distribution of the civil liability of employees, which is extended to the employer, *cf.* Art. 55 para. 1 OR.

Nonetheless, this justification cannot fully apply for Art. 62 nDSG which explicitly addresses private persons gaining knowledge of data whilst practicing their profession. Moreover, the expanded professional secrecy for private entities amounts to a prohibition of breaches of official secrecy (which until now was only applicable for public servants), thus obstructing whistle-blowers and other employees.[503]

e. Procedural Aspects

Priority of data regulation enforcement; equipment of enforcers; shaming impact of breaches.

Data protection enforcement under the oDSG must overcome many hurdles: the EDÖB has rather few areas of responsibility and most importantly can issue only recommendations. If he looks to enforce this guidance bindingly, he must apply to the administrative court in case of non-compliance. This detour makes the EDÖBs powers slower, costlier, and less efficient. In addition, the focus of the (written) sanction system of the oDSG lies on criminal prosecution and yet in practice only extremely few criminal judgements can be found in the field of data protection.[504]

The nDSG looks to overcome some of these **enforcement deficits** by most notably giving the EDÖB the power to issue binding rulings instead of recommendation and connecting non-compliance to a criminal sanction. Even though criminal provisions were sharpened, the nDSG does not lift the administrative burden of prosecution from the shoulders of cantonal criminal prosecution authorities – who are not only busy with regular criminal prosecution but moreover **alien to the subject of data protection**[505] – which is why

499 Eidgenössisches Bundesamt für Justiz, 'Vernehmlassungsverfahren nDSG' (n 155) 50.

500 Verband Schweizerischer Kantonalbanken, 'Detaillierte Bemerkungen zum Vorentwurf Datenschutzgesetz (VE-DSG)' (4 April 2017) 45; Verband des Schweizer Versandhandels, 'Vernehhmlassungsantwort zum Gesetzesentwurf Totalrevision Datenschutzgesetz' (30 March 2017) 4.

501 Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 6974, 7099.

502 ibid 6974.

503 Digitale Gesellschaft, 'Vernehmlassungsantwort: Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)' (30 March 2017) 20; grundrechte.ch, 'Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)' (4 April 2017) 13.

504 Rosenthal, 'Entwurf des nDSG' (n 229) 35; Pärli, 'Art. 34' (n 498) 380 et seq. with further proof.

505 Amongst many Rosenthal, 'Das neue Datenschutzgesetz' (n 37) 70; Appenzell Ausserrhoden, 'Eidg. Vernehmlassung; Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz - Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union; Stellungnahme des Regierungsrates von Appenzell Ausserrhoden' (31 March 2017) 11; Kanton Solothurn, 'Vernehmlassung zum Vorentwurf zum Bundesgesetz über die

a higher quota of criminal judgements is not to be expected. The answer to this particular deficit would be the introduction of administrative sanctions, which again was categorically rejected by the Federal Council, arguing that such sanctioning systems are traditionally used in Switzerland only for some economic areas subject to special concession (like postal services or gambling) or in the area of antitrust law.[506] Further, Art. 51 nDSG grants the EDÖB comprehensive possibilities to issue rulings controllers, a violation of which can be criminally prosecuted. Thus, the EDÖB gains ***de facto* regulatory power**.[507] **Nationwide uniform enforcement** of data protection law by a single body remains impossible under the nDSG nonetheless.

Totalrevision des Datenschutzgesetzes und die Änderungen weiterer Erlasse zum Datenschutz' (4 April 2017) 8.

[506] Schweizerischer Bundesrat, 'Botschaft zum nDSG' (n 10) 7098. He also raises the argument that the pecularity of corporate criminal liability makes the fundamental decision in Art. 102 para. 1 StGB to punish companies directly only in the case of specific organisational culpability and not sweepingly as would be the case with administrative sanctions, see also *supra* C.IV.3.c.

[507] ibid 7092.

D. Sources and Literature

Table of Cases

31 II 242, [1905] (BGE).

90 II 351, [1926] (BGE).

80 II 136, [1954] (BGE).

90 II 461, [1964] (BGE).

95 II 481, [1969] (BGE).

97 II 97, [1971] (BGE).

109 II 353, [1983] (BGE).

114 II 388, [1987] (BGE).

114 IV 46, [1988] (BGE).

119 II 443, [1993] (BGE).

121 III 31, [1995] (BGE).

122 III 449, [1996] (BGE).

126 III 305, [2000] (BGE).

130 III 28, [2003] (BGE).

5C.57/2004, [2004] (BGer).

133 III 153, [2006] (BGE).

A-3908/2008, [2009] (BVGer).

136 II 508, [2010] (BGE).

138 III 411, [2012] (BGE).

A-3831/2012, [2012] (BVGer).

138 III 425, [2012] (BGE).

140 I 2, [2014] (BGE).

141 III 265, [2015] (BGE).

4A_518/2020, [2020] (BGer).

References

Appenzell Ausserrhoden, 'Eidg. Vernehmlassung; Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz - Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union; Stellungnahme des Regierungsrates von Appenzell Ausserrhoden' (31 March 2017).

Baeriswyl B, 'Art. 29' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

—— 'Art. 4' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

—— 'Entwicklungen im Datenschutzrecht: Berichtszeitraum 1. Juli 2018 bis 30. Juni 2019' (2019) 115(19) SJZ 592.

BAKOM BfK, 'Bekämpfung der Internetkriminalität' (29 April 2022) <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html> accessed 29 April 2022.

Berger E, 'Deutscher Rechtskreis' (29 May 2022) <http://ieg-ego.eu/de/threads/crossroads/rechtsraeume-rechtskreise/elisabeth-berger-deutscher-rechtskreis> accessed 29 May 2022.

Bieri A and Powell J, 'Die Totalrevision des Bundesgesetzes über den Datenschutz' [2020] Jusletter.

Bieri P, 'Die Gerichte der Schweiz – eine Übersicht' [2014] Justice - Justiz - Giustizia.

Bradford A, The Brussels effect: How the European Union rules the world (Oxford University Press 2019).

Brehm R, Berner Kommentar: Kommentar zum schweizerischen Privatrecht; Schweizerisches Zivilgesetzbuch (5. Auflage, Stämpfli 2021).

Bühlmann L and Metin H, 'Totalrevision des Schweizer Datenschutzgesetzes vor dem Hintergrund der DS-GVO' (2019) 9(8) Zeitschrift für Datenschutz 356.

Bühlmann L and Reinle M, 'Neues Schweizer Datenschutzrecht: Wichtigste Regelungen Der DSG-Revision Im Überblick' mondaq (9 December 2020) <https://www.mondaq.com/privacy-protection/1014308/neues-schweizer-datenschutzrecht-wichtigste-regelungen-der-dsg-revision-im-berblick> accessed 25 March 2022.

Bühlmann L and Schüepp M, 'Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht' [2021] Jusletter <https://jusletter.weblaw.ch/juslissues/2021/1059.html> accessed 31 May 2022.

Bundesamt für Justiz, 'Stärkung des Datenschutzes' (24 March 2022) <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> accessed 24 March 2022.

Busse C-D, Die Methoden der Rechtsvergleichung im öffentlichen Recht als richterliches Instrument der Interpretation von nationalem Recht (Nomos Verlagsgesellschaft 2015).

daten:recht – das Datenrechts-Team von Walder Wyss, 'revDSG (revidierte Fassung mit Botschaft)' (23 May 2022) <https://datenrecht.ch/rev-dsg/> accessed 3 June 2022.

Digitale Gesellschaft, 'Vernehmlassungsantwort: Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)' (30 March 2017).

Drechsler C, 'Plädoyer für die Abschaffung des Datenschutzes für juristische Personen' (2016) 11(1) AJP 80-88.

EDÖB, 'Empfehlung des EDÖB betreffend Bonusprogramm Helsena+ der Helsena Zusatzversicherungen AG' (Bern 26 April 2018) A2018.04.13-0001.

—— 'Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG' (Bern 8 September 2020).

—— 'Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug (nach Art. 6 Abs. 2 lit. a) DSG)' (18 June 2021).

—— 'Stand des Datenschutzes weltweit' (15 November 2021).

—— 'Datareg 3.2 - WebDatareg' (21 April 2022) <https://www.datareg.admin.ch/> accessed 21 April 2022.

—— 'Stand der Produkt- und Dienstleistungszertifizierung' (19 May 2022) <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung/stand-der-produkt--und-dienstleistungszertifizierung.html> accessed 19 May 2022.

—— 'Zentralisierung von Human Resources im Ausland' (3 June 2022) <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/18--taetigkeitsbericht-2010-2011/zentralisierung-von-human-resources-im-ausland.html> accessed 3 June 2022.

Egli P, Introduction to Swiss Constitutional Law (DIKE 2016).

Eidgenössisches Bundesamt für Justiz, 'Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz' (21 December 2016).

—— 'Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz: Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens' (10 August 2017).

Epiney A, 'Vertraglicher «Umsetzungsdruck» und «autonomer Anpassungszwang» aus Brüssel' [2014] LeGes - Gesetzgebung und Evaluation 383.

EPO, 'Member states of the European Patent Organisation' (25 May 2022) <https://www.epo.org/about-us/foundation/member-states.html> accessed 25 May 2022.

Facebook [2020] KVR 69/19, [2020] 73 Gewerblicher Rechtsschutz und Urheberrecht 1318-1331 (BGH).

Federal Council, 'Institutional agreement' (8 June 2022) <https://www.eda.admin.ch/europa/en/home/europapolitik/ueberblick/institutionelles-abkommen.html> accessed 8 June 2022.

Gaba 2C_180/2014, [2016] (BGE).

Geiser T, Die Persönlichkeitsverletzung insbesondere durch Kunstwerke (Basler Studien zur Rechtswissenschaft Reihe A vol 21, Helbing & Lichtenhahn 1990).

George D, 'Juristische Personen als Subjekte der Datenschutzgesetzgebung' [2016] Jusletter.

Google Street View 138 II 346, [2012] (BGE).

Gratwohl N and Höltschi R, 'Facebook: Deutsches Bundeskartellamt setzt Grenzen' Neue Zürcher Zeitung (7 February 2019) <https://www.nzz.ch/wirtschaft/facebook-deutsches-bundeskartellamt-setzt-grenzen-ld.1458137> accessed 30 May 2022.

Griesinger M, 'Ein Überblick über das neue Schweizer Datenschutzgesetz (DSG)' [2021] Privacy in Germany 43.

grundrechte.ch, 'Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)' (4 April 2017).

Hartford Fire Ins. Co. v. California 509 U.S. 764, [1993] (United States Supreme Court).

Helsana+ A-3548/2018, [2019] (BVGer).

Hennemann M, 'Das Schweizer Datenschutzrecht im Wettbewerb der Rechtsordnungen' in Boris P Paal, Dörte Poelzig and Oliver Fehrenbacher (eds), Deutsches, europäisches und vergleichendes Wirtschaftsrecht: Festschrift für Werner F. Ebke zum 70. Geburtstag (C.H. Beck 2021).

Hilty RM, '§ 58 Schweiz' in Ulrich Loewenheim (ed), Handbuch des Urheberrechts (Beck-Online Bücher, 3. Auflage. C.H. Beck 2021).

Jutzi T, 'Der Einfluss des EU-Rechts auf das schweizerische Recht der kollektiven Kapitalanlagen' (2015) 6(1) Aktuelle Juristische Praxis 1.

Kanton Aargau, 'Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassung' (22 September 2021).

Kanton Bern, 'Vernehmlassung des Bundes: Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Stellungnahme des Kantons Bern' (15 September 2021).

Kanton Solothurn, 'Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderungen weiterer Erlasse zum Datenschutz' (4 April 2017).

Killias L, Kramer M and Rohner T, 'Gewährt Art. 158 ZPO eine "pre-trial discovery" nach US-amerikanischem Recht' in Franco Lorandi and Daniel Staehelin (eds), Festschrift für Ivo Schwander (DIKE 2011).

Körber T, 'Art. 1 FKVO' in Ulrich Immenga and others (eds), Wettbewerbsrecht (6. Auflage. C.H. Beck 2019).

Kunz PV, 'Europa als ein Massstab für das schweizerische Wirtschaftsrecht?: Rechtsvergleichende Fragestellungen zu einem "Weg nach Europa" anhand des neuen Kollektivanlagenrechts' in Wolfgang Wiegand and Hans P Walter (eds), Tradition mit Weitsicht: Festschrift für Eugen Bucher zum 80. Geburtstag (Stämpfli; Schulthess 2009).

—— 'Instrumente der Rechtsvergleichung in der Schweiz bei der Rechtssetzung und bei der Rechtsanwendung' [2009] Zeitschrift für Vergleichende Rechtswissenschaft 31.

Langhanke C, 'Datenschutz in der Schweiz: Reichweite der europarechtlichen Vorgaben' (2014) 4(12) Zeitschrift für Datenschutz 621.

Lemmens K, 'The Protection of Privacy between a Rights-Based and a Freedom-Based Approach: What the Swiss Example Can Teach Us' (2003) 11(3) Tilburg Foreign Law Journal 605.

Leuenberger C and Uffer-Tobler B, Schweizerisches Zivilprozessrecht (2nd edn, Stämpfli 2016).

Meili A, 'Art. 28' in Thomas Geiser and Christiana Fountoulakis (eds), Zivilgesetzbuch I: Art. 1 - 456 ZGB (Basler Kommentar vol 1, 6th edn. Helbing & Lichtenhahn 2018).

—— 'Art. 28a' in Thomas Geiser and Christiana Fountoulakis (eds), Zivilgesetzbuch I: Art. 1 - 456 ZGB (Basler Kommentar vol 1, 6th edn. Helbing & Lichtenhahn 2018).

Metille S, 'Swiss Information Privacy and the Transborder Flow of Personal Data' (2013) 8(1) Journal of International Commercial Law and Technology 71.

Minelli 127 III 481, [2001] (BGE).

Morand A-S and Duc S, 'International data transfers and the EU's adequacy decisions' [2021] Jusletter.

Oberlin JS and Kessler R, 'Daten: Die Schlüsselrolle im Kampf gegen die Coronavirus-Pandemie?' [2020] Jusletter.

Oesch M, 'Die bilateralen Abkommen Schweiz-EU und die Übernahme von EU-Recht' [2017] Aktuelle Juristische Praxis (AJP) 638.

Pärli K, 'Art. 34' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

—— 'Art. 35' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

Peter C, 'Das Begehren um Löschung von Patientendaten' [2019] Jusletter.

Pfaff I, 'Suisse Secrets: Wie die Schweiz auf die Enthüllungen reagiert' Süddeutsche Zeitung (21 February 2022) <https://www.sueddeutsche.de/wirtschaft/suisse-secrets-schweiz-credit-suisse-bankgeheimnis-1.5533261> accessed 26 March 2022.

Powell J, 'Die Revision der kantonalen Datenschutzgesetze' [2021] Jusletter.

privatim, 'Home-Seite' (24 March 2022) <https://www.privatim.ch/de/home-page/> accessed 24 March 2022.

Rehm GM, 'Rechtstransplantate als Instrument der Rechtsreform und -transformation' (2008) 72(1) The Rabel Journal of Comparative and International Private Law 1.

Rosenthal D, 'Der Entwurf für ein neues Datenschutzgesetz' [2017] Jusletter.

—— 'Das neue Datenschutzgesetz' [2020] Jusletter.

Rosenthal D and Jöhri Y, Handkommentar zum Datenschutzgesetz (Schulthess 2008).

Rudin B, 'Art. 3' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

Schmid A, Schmidt KJ and Zech H, 'Rechte an Daten - zum Stand der Diskussion' (2018) 21(11) sic! Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 627.

Schrems II C-311/18, [2020] (ECJ).

Schwaibold M, 'Art. 28g' in Thomas Geiser and Christiana Fountoulakis (eds), Zivilgesetzbuch I: Art. 1 - 456 ZGB (Basler Kommentar vol 1, 6th edn. Helbing & Lichtenhahn 2018).

Schweizerische Lauterkeitskommission SLK, 'Entscheid Nr. 179/16' (23 November 2016).

Schweizerischer Bundesrat, 'Botschaft über die Änderung des Schweizerischen Zivilgesetzbuches: Persönlichkeitsschutz: Art. 28 ZGB und 49 OR' (1982) 133(28) Bundesblatt 636.

—— 'Botschaft zum Bundesgesetz über den Datenschutz (DSG)' (1988) 139(18) Bundesblatt 413.

—— 'Botschaft zu einem Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG), zu einem Bundesgesetz über den Schutz von Topographien von integrierten Schaltungen (Topographiengesetz, ToG) sowie zu einem Bundesbeschluss über verschiedene völkerrechtliche Verträge auf dem Gebiete des Urheberrechts und der verwandten Schutzrechte vom 19. Juni 1989' (1989) 140(39) Bundesblatt 477.

—— 'Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung

personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung' (2003) 154(10) Bundesblatt 2101.

—— 'Botschaft zur Schweizerischen Zivilprozessordnung (ZPO)' (2006) 157(37) Bundesblatt.

—— 'Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz' (2017) 168(45) Bundesblatt 6941.

Schwenzer I, 'Development of Comparative Law in Germany, Switzerland, and Austria' in Mathias Reimann and Reinhard Zimmermann (eds), The Oxford handbook of comparative law (Second edition. Oxford University Press 2019).

Stark J, Interview with David Rosenthal (24 November 2021).

Sturny M, 'Facebook-Entscheid des Bundeskartellamts zu Nutzerdaten' (30 May 2022) <https://datenrecht.ch/facebook-entscheid-des-bundeskartellamts-zu-nutzerdaten/> accessed 30 May 2022.

Sury U, 'Das neue Datenschutzgesetz der Schweiz im Vergleich zur DSGVO' (2021) 44(3) Informatik Spektrum 221.

SVP, 'Eröffnung des Vernehmlassungsverfahren: Antwort der Schweizerischen Volkspartei (SVP)' (4 April 2017).

Tobler S, 'Warum die Schweiz ihr Bankgeheimnis verlor' in Mark Eisenegger, Linards Udris and Patrik Ettinger (eds), Wandel der Öffentlichkeit und der Gesellschaft: Gedenkschrift für Kurt Imhof (Springer Fachmedien Wiesbaden 2019).

Universität Bern, 'swiss votes' (9 May 2022) <https://swissvotes.ch/votes?page=0> accessed 9 May 2022.

Vasella D, 'Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht' [2015] Jusletter <https://jusletter.weblaw.ch/juslissues/2015/824/zur-freiwilligkeit-u_90937b2cfa.html>.

—— 'FAQ: DSGVO und neues Schweizer Datenschutzgesetz' (2021) <https://www.youtube.com/watch?v=wblMaaElIe8&t=1s> accessed 2 June 2022.

—— 'Revision des DSG: Bedeutung für international tätige Unternehmen' (16 June 2021) <https://www.youtube.com/watch?v=wblMaaElIe8&t=1s> accessed 3 June 2022.

Vasella D and Sievers J, 'Der "Swiss Finish" im Vorentwurf des DSG' [2017] digma - Zeitschrift für Datenrecht und Informationssicherheit 44.

Verband des Schweizer Versandhandels, 'Vernehhmlassungsantwort zum Gesetzesentwurf Totalrevision Datenschutzgesetz' (30 March 2017).

Verband Schweizerischer Kantonalbanken, 'Detaillierte Bemerkungen zum Vorentwurf Datenschutzgesetz (VE-DSG)' (4 April 2017).

Volkszählungsurteil [1983] 1 BvR 209/83, [1984] 37 Neue Juristische Wochenschrift 419 (BVerfG).

Waldmeier S-D, 'Informationelle Selbstbestimmung - ein Grundrecht im Wandel?' (University of Zurich 2015).

Wemelinger A, 'Art. 12' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

Wermelinger A, 'Art. 13' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

—— 'Art. 14' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

—— 'Art. 15' in Bruno Baeriswyl and Kurt Pärli (eds), Datenschutzgesetz (DSG) (Stämpfli Verlag 2015).

—— 'Vernehmlassungsvorlage Verordnung zum Bundesgesetz über den Datenschutz' [2021] Jusletter.

Wernicke S, 'Anmerkung zu EuGH, Urteil vom 6.9.2017 - C-413/14 P' [2017] Europäische Zeitschrift fürs Wirtschaftsrecht 850.

Wettbewerbskommission (WEKO), 'Jahresbericht 2016' .

—— 'Jahresbericht 2021' .

WIPO, 'Information by Country: Switzerland' (25 May 2022) <https://www.wipo.int/directory/en/details.jsp?country_code=CH> accessed 25 May 2022.

Zanon NB and Boccali O, 'Die neue Schritt-für-Schritt-Anleitung zur Übermittlung von Personendaten ins Drittland nach Schweizer Datenschutzrecht' [2022] Privacy in Germany 40.

Zweigert K and Kötz H, Einführung in die Rechtsvergleichung: Auf dem Gebiete des Privatrechts (Mohr 1996).