Data access rights – A comparative perspective

Louisa Specht-Riemenschneider

A. Introduction

I. From data ownership to data access

Discussion about data access rights has replaced discussion of data ownership, at least among German academics. For quite a long time, experts debated whether there could be data ownership or other exclusive rights to data.[1] Most importantly, some scholars emphasised the legal uncertainty that could arise in that if the existence of such rights is rejected. Based on this argument one can reason that exclusive rights in data are necessary. Nevertheless, the introduction of such exclusive rights could lead to a strengthening of technically established power over data if the person technically controlling the data becomes the data owner. On the other hand, if an exclusive right to data is established to overcome technical control over data, e.g. by granting data ownership to the party suffering detriment from technical control by another party, data ownership may not be the correct description of the legal instrument that needs to be introduced. If a party other than the technical data controller is to be allowed to access data and use it, that party would be granted a "data access right".

II. Functional taxonomy of data access rights

Data access rights exist to varying degrees in different legal systems. These rights differ with regard to their function. Data access can be granted in two ways: Firstly, data access can be granted by virtue of disclosure obliga-

1 Fundamental: Herbert Zech, *Information als Schutzgegenstand* (Mohr Siebeck 2012). See also Louisa Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit Schutzbereich, Alternativen' (2016) Computer und Recht 288; Wolfgang Kerber and Louisa Specht-Riemenschneider, 'Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland-USA' (ABIDA 2017) <www.abida.de/en/node/426> accessed 31 August 2020.

tions without the requirement of filing a request, such as pursuant to Sections 3 and 12a of the German E-Government Act (*E-Government-Gesetz*) and the transparency laws of certain German federal states.[2] These disclosure obligations are intended to create transparency on the part of the government and the administration with regard to basic information. Secondly, data access can be granted upon request. These data access rights encompass more and other data than the data available pursuant to disclosure obligations, and requests may be declined for certain reasons, for example if third-party rights may be infringed if data access is provided. In this paper, the current debate on data access is primarily of interest with regard to how data access rights pursuant to a request can overcome technical power over data (i.e. 'genuine access rights').

Sub-categories of genuine access rights can be recognised regarding the functioning of the access rights. Genuine data access rights exist under contract law, where they are recognised because of information asymmetries, on the one hand, and also under antitrust law, where their purpose is to curb abuse of market power. The function of the third type of data access right is to overcome technical power over data without requiring constraint of market power, and without affecting contracts between the applicant and the data controller. This type of data access right is the focus of this paper.

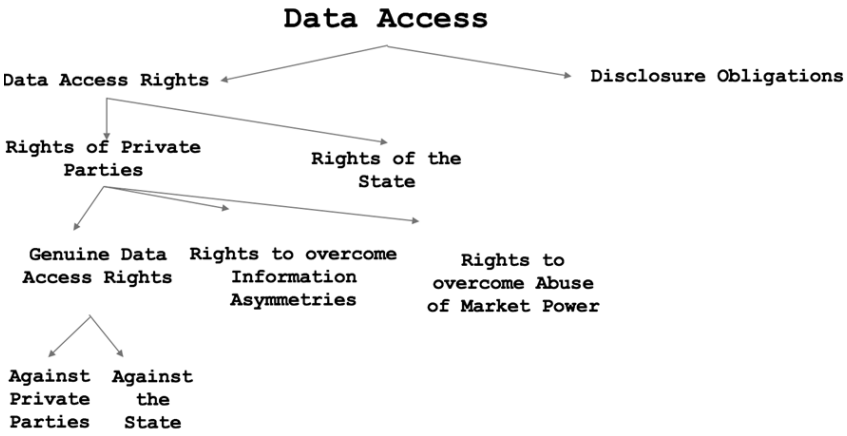
Genuine data access rights that serve to overcome technical power over data without regard to contract law and antitrust law can in turn be subcategorised according to function. Rights can be directed against the state, as guaranteed for example under the Public Sector Information Directive, or directed against private individuals. Data access rights directed against private individuals are the sole concern here, as data access rights directed against the state are the subject of a different chapter of this volume. Lastly, claims for information regarding the infringement of intellectual property rights and personality rights are also excluded because these have a special function, the regulation of which is not within the scope of this paper.

In some jurisdictions, such as France, there are also data access rights which accrue to governments and administrations and are directed against

2 An overview can be found at Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 257; Josef Drexl and others, 'Data Ownership and Access to Data', Max Planck Institute for Innovation and Competition (2016) ≤www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf> accessed 31 August 2020.

private individuals. These data access rights of governments and administrations will be examined in another chapter of the conference proceedings, too.

Fig. 1 – Functional taxonomy of data access rights



The question to be discussed in the context of comparative law is therefore: How are data access rights in relationships between private individuals – apart from contractual information asymmetries, infringements of intellectual property rights and personality rights and abuse of market power – guaranteed in the various legal systems?

B. Course of investigation

This question is to be examined in steps, following the elaboration of the specific question to be discussed. The first step in the comparative law method is to look at how the defined problem is solved in national law. I will not go into detail concerning national law, as the other papers in this volume will shed light on national law and its various guarantees of data access rights. I will therefore only briefly describe the instruments with which data access rights against private individuals are guaranteed, apart from contractual information asymmetries and the abuse of market power, before categorising these particular instruments.

Within this taxonomy, I will group the relevant foreign laws to point out the countries that guarantee data access rights in a manner similar to German law and which countries have chosen to recognise different data access rights. I will present these different data access rights and explain which similar foreign data access rights, in my opinion, have advantages over the data access rights existing under German law. I will also explain why certain other legal systems have chosen to recognise different data access rights than Germany has, and finally I will summarise my findings and derive policy recommendations from my research.

C. *National law: Taxonomy of data access rights*

The law in Germany grants data access rights in two ways, essentially: 'sole access' to data, which is processed by the controller, pursuant for example to Article 15 GDPR[3], and by way of a right to data portability, which covers the right to receive the data in a structured, commonly used and machine-readable format, as per Article 20 GDPR, for example. This is the primary finding. The second relevant finding regarding the categorisation taxonomy of data access rights under national law is that data access rights are guaranteed either for a specific sector or for a specific type of data. Conversely, there are no data access rights that are guaranteed across sectors or data types. Sector-specific data access rights can be found, for example, in Article 6 of Regulation (EC) 715/2007 which grants access to vehicle repair and maintenance information.[4]

The PSD2 Directive[5] also provides for a data access right in the banking sector. According to Article 67 of this directive, banks in the EU are required to open customer interfaces for third-party providers and grant these providers access to bank accounts. One difference versus data porta-

3 Regulation (EU) No. 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 Regulation (EC) No. 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions form light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information [2007] OJ L171/1.

5 Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L335/36.

bility under the GDPR is that PSD2 regulates access to interfaces which are to be connected with each other at all times. The right to data portability, in contrast, concerns a single release of data only.

Another sector-specific data access right is provided for in Article 16(4) of the Digital Content Directive, which is to be transposed into national law. It reads:

> Except in the situations referred to in point (a), (b) or (c) of paragraph 3, the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader.
> The consumer shall be entitled to retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format.

For the healthcare sector a sector-specific right of access to data is provided for in Section 630g of the German Civil Code (BGB), according to which the right holder has the right to access his or her patient file. In requiring mobile number portability, Section 46(3) of Germany's Telecommunications Act (*Telekommunikationsgesetz*) contains a right to data portability too, whereas Article 20 GDPR grants a cross-sector right to data portability. The data access rights provided for under Article 15 GDPR and Section 34 of Germany's Federal Data Protection Act (BDSG) also apply on a non-sector-specific basis. The rights cited here do not represent an exhaustive list of all existing data access rights, being intended rather to illustrate that data access rights may apply in specific sectors or be guaranteed across sectors.

Beyond classifying data access rights as sector-specific or non-sector-specific, data access rights can also be categorised as concerning specific data, such as personal data only, or concerning both personal and non-personal data. It is important to note that Germany's cross-sectoral data access rights are limited to personal data, while sector-specific rights are partly guaranteed for both personal and non-personal data. Thus there is no cross-sectoral, non-type-specific data access right, and there is no sector-specific right of access to personal data. However, German and European law do not require a sector-specific solution concerning personal data, because the GDPR exhaustively permits the processing of personal data across all sectors.

Fig. 2 – Classification of data access legislation

	sector-specific regulation	cross-sectoral regulation
data-specific regulation		Art. 15, 20 DSGVO, § 34 BDSG; Art. 16 (4) Digital Content Directive
cross-type of data regulation	Art. 6 VO 715/2007 Art. 67 PSD2 Directive § 46 (3) TKG	

D. Foreign legal systems: Taxonomy of data access rights, comparison with German law

There are three aspects of foreign data access rights of primary interest:

1. Does a foreign law system provide for data access rights that are guaranteed across sectors and data types?
2. If a foreign law system provides for sector-specific data access rights, what do these look like? What sectors are concerned? Who enjoys the right guaranteed? What requirements have to be met to obtain data access? What legal consequences are provided for if data access is unlawfully denied? Is the data right transferable, and does compensation have to be paid? What limitations apply?
3. If there are cross-sectoral regulations in foreign legal systems similar to the GDPR, in what points do the envisaged data access rights differ from the provisions of the GDPR, and why? What ideas from foreign legal systems could be incorporated into the GDPR, which is currently under evaluation?

The legal systems of the following states are taken into consideration, as they provide for substantial genuine data access rights:

- USA and California separately
- Brazil
- Australia
- Japan
- India
- New Zealand
- The Philippines
- Singapore
- Switzerland
- France
- Post-Brexit UK

Examining these different jurisdictions, it turns out that most of them provide for data access rights similar to the GDPR, which means they provide for cross-sectoral data access rights that are limited to personal data. I will thus provide an overview of the deviations from the GDPR in the various legal systems, taking a special look at New Zealand and the Philippines, whose regulations could possibly serve as a model.

The US provides for data protection in specific sectors only, primarily healthcare and banking, and the UK, as the Furman Report shows, is looking to follow a similar path. The UK's Personal Data Mobility Act would in any case limit the right to data portability to individual sectors, but it has not yet been enacted.[6]

Much in contrast, France has established very far-reaching data access rights that are designed to apply across sectors and data types. Australia guarantees a data access right across data types in the banking sector only, but this is to be extended to other sectors.

The article was written in December 2019 and is therefore on the status of the legislation at that time. However, Australian law has changed so fundamentally since then, and at the same time it contains such important new provisions that could be considered as model provisions for European law, that Australian law has been brought up to date to January 2021, the date of the final corrections.

---

6 Jason Furman and others, 'Unlocking digital competition – Report of the Digital Competition Expert Panel' (2019) 66 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 31 August 2020.

I. Sectoral data protection regulation

The United States has established specific data access rights for the healthcare and banking sectors in the Health Insurance Portability and Accountability Act (HIPAA) and the Consumer Protection Principles (CPP) and for minors in the Children Online Privacy Protection Act (COPPA).

1. HIPAA

Section 164.524 HIPAA provides for a right to access protected health information:

> (1) Right of *access*. Except as otherwise provided [...], an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:
> (i) Psychotherapy notes; and
> (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
> (iii) Protected health information maintained by a covered entity [...][7]

This right basically corresponds to the right to information per Section 630g German Civil Code (*Bürgerliches Gesetzbuch*), and with the exception of the limited circle of addressees and certain other details, also corresponds essentially to Article 15 GDPR. There are reviewable and unreviewable grounds for denial, and the covered entity may impose a reasonable cost-based fee.

2. COPPA

The Children Online Privacy Protection Act (COPPA) provides for a very basic right to information for minors. In Section 1303(b) it states that

> (1) In General.–Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate [...] regulations that

7 Emphasis added.

> (B) require the operator to *provide*, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent –
> (i) a description of the specific types of personal information collected from the child by that operator;
> (ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and
> (iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child.[8]

According to COPPA, the website operator neither has a duty to inform the child about the personal data gathered, in detail, nor is the operator obliged to act within a defined period. However, children can of course exercise the comprehensive information rights under the CCPA, which will be discussed in detail later on.

3. CPP

The Consumer Protection Principles are intended to reiterate the importance of consumer interests in the developing market for consumer-authorised use of financial data. The Principles are designed to ensure that markets for consumer financial products and services are fair, transparent and competitive. Consumers are to be afforded protection, utility and value.[9] The CPPs are implemented and enforced by the Consumer Finance Protection Bureau as its mission, defined by the US Congress in the Dodd-Frank Act.[10]

---

8 Emphasis added.

9 Consumer Financial Protection Bureau, 'Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation' (2017) <https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf> accessed 31 March 2020.

10 Dodd-Frank Wall Street Reform and Consumer Protection Act <https://legcounsel.house.gov/Comps/Dodd-Frank%20Wall%20Street%20Reform%20and%20Consumer%20Protection%20Act.pdf> accessed 21 March 2020; Consumer Financial Protection Bureau, 'Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation' (2017) <https://files.consumerfinance.gov/

Principles 1 and 2 provide for:

1) Access
Consumers are able, upon *request*, to *obtain information* about their ownership or use of a financial product or service from their product or service provider. Such information is made available in a timely manner. Consumers are generally able to authorize trusted third parties to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner.
Financial account agreements and terms support safe, consumer-authorized access, promote consumer interests, and do not seek to deter consumers from accessing or granting access to their account information. Access does not require consumers to share their account credentials with third parties.
2) Data Scope and Usability
Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards. Information is made available in forms that are readily usable by consumers and consumer-authorized third parties. Third parties with authorized access only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary.

The main difference between the data access rights per the GDPR and per Principles 1 and 2 of the CPP is the possibility for third parties to exercise the right. With regard to Article 20 GDPR this has been much discussed.[11]

---

f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf> accessed 31 March 2020.

11 Tim Jülicher, Charlotte Röttgen and Max von Schönfeld, 'Das Recht auf Datenübertragbarkeit' (2016) Zeitschrift für Datenschutz 358, 360; Carlo Piltz, 'Die Datenschutz-Grundverordnung' (2016) Kommunikation & Recht 629, 634; Moritz Hennemann, 'Datenportabilität' (2017) Privacy in Germany 5, 6; Sebastian Brüggemann, 'Das Recht auf Datenportabilität' (2018) Kommunikation und Recht 1; Tim Sperlich, 'Das Recht auf Datenübertragbarkeit' (2017) Datenschutz und Datensicherheit 377; Michael Strubel, 'Anwendungsbereich des Rechts auf Datenübertragbarkeit' (2017) Zeitschrift für Datenschutz 355, 356; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung/Bundesdatanschutzgesetz* (2nd edn, C.H. Beck 2018) Art. 20 DS-GVO para. 1, 19; Wulf Kamlah, in Kai-Uwe Plath (ed.), *DSGVO/BDSG* (3rd edn, Otto Schmidt 2018) Art. 20 DS-GVO paras 2–3; Matthias Rudolph, in Rolf Schwartmann and

II. Cross-sectoral data protection regulation

1. California

California takes a leading role in protecting privacy in the US. Although data protection and privacy protection are not exactly the same, as data protection is an aspect of privacy as interpreted in relation to Article 8 of the European Convention on Human Rights (ECHR),[12] the California privacy protection regime also focuses on prohibitions of data processing and on the rights of data subjects, including data access and data portability rights in particular. As the most detailed privacy regime within the US, another reason for its major importance is that most prominent tech companies are located in Silicon Valley and thus are subject to these quite stringent laws. Enacted in January 2020, the California Consumer Privacy Act (CCPA) has set even higher privacy protection standards than under previous laws.[13] Pursuant to California Civil Code Section 1798.145(a)(6) and Section 1798.140(c)(1), companies doing business in California have to comply with the CCPA. An exemption only applies if a company has an annual revenue of less than US$ 25 million, collects data from fewer than 50,000 Californians annually and earns less than 50 % of its income from data commerce.[14] The Assembly Bills 25 and 1355 exempt certain data, such as employee data and business communication data, from the scope of application of the CCPA until the first of January 2021.[15] Assembly Bill 874 clarifies that 'personal information' includes information that reasonably identifies, relates to, describes or can reasonably be associated with a

---

others (ed.), *DS-GVO/BDSG* (C.F. Müller 2018) Art. 20 DSGVO para. 24; Louisa Specht-Riemenschneider and Linda Bienemann, 'Datenübertragbarkeit anleger- und anlagerelevanter Daten' in Dimitrios Linardatos (ed.), *Rechtshandbuch Robo Advice* (Vahlen 2020) § 11 Rn. 7; Kai von Lewinski, in Heinrich A. Wolff und Stefan Brink (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (31st edn, C.H. Beck 2020) Art. 20 DSGVO para. 7, 113–114; Article 29 Working Party, 'Guidelines on the right to data portability' (5 April 2017) 3 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44095> accessed 31 August 2020.

12 Christoph Grabenwarter and Katharina Pabel, *Europäische Menschenrechtskonvention* (6th edn, C.H. Beck 2016) § 22 Rn. 9–10; Christina-Maria Leeb and Johannes Liebhaber, 'Grundlagen des Datenschutzrechts' (2018) Juristische Schulung 534, 535.

13 Lothar Determann, 'Kalifornisches Gesetz gegen Datenhandel' (2018) Zeitschrift für Datenschutz 443, 444.

14 Ibid.

15 Axel Spies, 'Änderungen und Klarstellungen zum California Consumer Privacy Act (CCPA) beschlossen' (2019) Zeitschrift für Datenschutz-Aktuell 06781.

particular consumer or household, or could reasonably be associated, directly or indirectly, with a particular consumer or household.[16] Thus the concept of personal information is largely identical with the concept of personal data under the GDPR.

The CCPA is quite similar to the GDPR, although there are some differences.[17] With regard to data access rights these differences are elaborated here in detail:

California Civil Code Section 1798.100 provides that

> (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.
> (b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.
> (c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.
> (d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.
> (e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

16 Ibid.
17 Regarding these differences see Determann (n. 13) 446.

(1) Retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business.
(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

Section 1798.100 is specified by Section 1798.110, which gives detailed information about what data has to be disclosed to the consumer, such as the categories of personal data collected about the consumer, the categories of sources from which personal data are collected, the business or commercial purpose for collecting or selling personal data, the categories of third parties with whom the business shares personal data, and, most importantly, the specific personal data the business has collected about a given consumer.

Section 1798.100 is furthermore specified by Section 1798.130, which states, highly significantly, that a business has to disclose and deliver the mandatory data to the consumer free of charge within 45 days of receiving a verifiable request from the consumer. The GDPR requires the data subject to be informed without delay, within one month at the latest, which means that the GDPR is much stricter in its details. According to the CCPA, the disclosure must cover the 12-month period prior to receipt of the verifiable request by the business, whereas under the GDPR the data controller is required to disclose all personal data received to date.

Section 1798.100 in conjunction with Section 1798.110 is to be qualified as a cross-sectoral right to disclose personal data, but it also provides for a right to data portability in Section 1798.100 item d. in conjunction with Section 1798.130 (2). The section refers to all personal data collected, collection being defined as 'buying, renting, gathering, obtaining, receiving or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior' – see Section 1798.140 item e.

The right does not only cover information being given by the consumer but also the information being gathered without the consumer recognising the data collection.[18] The wording could also be interpreted to cover derived data if derived data are interpreted as being part of observation data. This remains unclear. Section 1798.100. in conjunction with Sections 1798.110 and 1798.130 requires a verified request, whereas Article 15

18 Thomas Hoeren and Stefan Pinelli, 'Das neue kalifornische Datenschutzrecht am Maßstab der DS-GVO' (2018) Multimedia und Recht 711, 714.

GDPR only requires a verified request in case of doubt; see Article 12(1) and (6) GDPR. Section 1798.100 does not require a business to retain any personal data collected for a single, one-time transaction if 'such data is not sold or retained by the business, or to reidentify or otherwise link to information that is not maintained in a manner allowing it to be considered personal information'. A similar exception is provided for in Art. 11 (1) GDPR. Lastly, it must be mentioned that a business is not required to provide personal information to a consumer more than twice within a 12-month period. Article 12(5) GDPR only provides that excessive requests may be rejected, the question of what is excessive being decided on a case-by-case basis. Section 1798.115 provides for another right to disclose data in cases where data are sold. More importantly, Section 1798.125 provides for a right to non-discrimination against consumers exercising consumer rights, such as by withholding products.[19] The GDPR does not provide for such a right. The following provision, which could serve as a model for Europe, is worth quoting in its entirety:

> 1798.125.
> (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:
> (A) Denying goods or services to the consumer.
> (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
> (C) Providing a different level or quality of goods or services to the consumer.
> (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
> (2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.
> (b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference

19 Determann (n. 13) 445.

> is directly related to the value provided to the business by the consumer's data.
> (2) A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130.
> (3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.
> (4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

Enforcement of the CCPA is the responsibility of the Office of the Attorney General of California.

2. New Zealand

New Zealand's privacy regime is principle-based, in contrast to the more prescriptive nature of the GDPR. The Privacy Bill is to repeal and replace the Privacy Act of 1993, as was recommended in the Law Commission's 2011 review of the Act, but it has not yet been adopted.[20] The Bill outlines 13 privacy principles, one of which is 'access to personal information'. This Privacy Principle 6 is to be qualified as a cross-sectoral right to information on personal data retained, similar to Article 15 GDPR. The Privacy Bill does not provide for a right to data portability. Such a right to data portability was proposed by the Privacy Commissioner in 2017,[21] and is considered by the majority of New Zealanders[22] to be important, though it was not included in the latest draft of the Privacy Bill dated March 2019.

---

20 Privacy Bill 2018 (34–2) <www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_77618/tab/digest> accessed 31 August 2020.

21 Privacy Commissioner/Te Mana Matapono Matatapu, 'Report to the Minister of Justice under Section 26 of the Privacy Act, Six Recommendations for Privacy Act Reform', para. 8 <www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26-of-the-Privacy-Act.pdf> accessed 31 August 2020.

22 Ibid. para. 10.

Principle 6 of the Privacy Act 1993 reads:

> (1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be
> (a) To obtain from the agency confirmation of whether or not the agency holds such personal information about them; and
> (b) To have *access* to that information. [...][23]

In Part 4 of the Privacy Bill, several details concerning Privacy Principle 6 are outlined, including chiefly the following:

> (46) A requestor may ask that an IPP 6 request be treated as urgent [...]
> (47) An agency must give reasonable assistance to an individual […]
> (48) (1) This section applies if an agency that receives an IPP 6 request
> (a) does not hold the information to which the request relates, but believes that the information is held by another agency; or
> (b) believes that the information to which the request relates is more closely connected with the functions or activities of another agency.
> (2) The agency must promptly, and in any case not later than 10 working days after the day on which the IPP 6 request is received, transfer the request to the other agency and inform the requestor accordingly.
> (3) However, subsection (2) does not apply if the agency has good cause to believe that the requestor does not want the request transferred to another agency.
> (50A) (1) If an agency grants access [it] must state
> (a) the way the information is made available;
> (b) the charge (if any) payable […];
> (c) the requestor's right to complaint to the Commissioner about the charge that is payable (if any).
> (50B) (1) An agency may refuse access to the personal information requested, only if the agency is able to rely on any of sections 52 to 57 […].
> (2) The notice given […] must state
> (a) the reason for the refusal; and
> (b) the requestor's right to make a complaint […].
> (50C) (1) An agency may neither confirm nor deny that it holds the personal information, [if it]

23 Emphasis added.

(a) is able to rely on section 52(1)(a)(i) or […]; and
(b) is satisfied that the interest protected by any of those provisions would be likely to be prejudiced by the agency confirming whether or not it holds the information about the requestor.
(52) (1) An agency may refuse access to any personal information requested if
(a) the disclosure of the information would—
(i) be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; or
(ii) create a significant likelihood of serious harassment of an individual; or
(iii) include disclosure of information about another person who—
(A) is the victim of an offence or alleged offence; and
(B) would be caused significant distress, loss of dignity, or injury to feelings by the disclosure of the information; or […]
(53) (1) An agency may refuse access […] if—
(a) the information is evaluative material and the disclosure of that information or of the information identifying the person who supplied it would breach an express or implied promise—
(i) that was made to the person who supplied the information; and
(ii) that was to the effect that the information or the identity of the person who supplied it, or both, would be held in confidence; or […]
(54) Security, defence, international relations as reason for refusing access to personal information […]
(55) Trade secret as reason for refusing access to personal information […]
(57) Other reasons for refusing access to personal information […]
(58) (2) Instead of refusing access to the personal information requested, the agency may grant access to the information, but may impose *conditions* relating to either or both of the following:[24]
(a) the requestor's use of the information:
(b) the requestor's disclosure of the information to any other person.
(61) (1) If the personal information requested is contained in a document and there is good reason under any of sections 52 to 57 for withholding some of that information, the agency may decide to grant the requestor access to a copy of that document under section 50(2) with any deletions or alterations in respect of the information that could be withheld that it considers necessary.

24 Emphasis added.

(72) (1) In relation to an IPP 6 request,—
(a) a public sector agency may, if authorised under section 73, impose a charge for making information available in compliance, in whole or in part, with the request:
(b) a private sector agency may, subject to the provisions of any applicable code of practice, impose a charge for—
(i) providing assistance under section 47, but only if the agency makes information available in compliance, in whole or in part, with the request:
(ii) making information available in compliance, in whole or in part, with the request.
(4) A charge […] must be reasonable and, […] may be had to—
(a) the cost of the labour and materials involved in making the information available; and
(b) any costs involved in making the information available urgently […].
(5) An agency may require all or part of a charge to be paid in advance.

Information Privacy Principle 6 has two chief advantages over Article 15 GDPR, the first of which is that the requestor may ask that an IPP 6 request be treated as urgent. If a request is designated as urgent, it must be treated as such by the controller. The second advantage over Article 15 GDPR is that IPP6 offers the possibility of providing data under terms and conditions instead of refusing access to the personal data requested. The possibility to erase and correct data before it is provided to the data subject is offered in Article 15 GDPR as well, following from a teleological interpretation of this provision, as it aims to provide comprehensive protection for the data subject, and it is more suitable for the data subject to receive abridged data than no data at all.

There are two other details which may be seen as advantageous or disadvantageous depending on one's point of view. IPP6 provides for an extensive and detailed catalogue of reasons for refusing to provide information on data, whereas Article 15(4) GDPR only states that the information provided must not infringe the rights of third parties. Any third-party rights qualify; Recital 63 cites trade secrets and intellectual property rights by way of example only, including particularly software copyrights. Article 15(4) GDPR requires that the rights and interests concerned be weighed in each individual case, therefore allowing for greater case-by-case justice, while IPP6 creates greater legal certainty due to the explicit enumeration of reasons for exclusion.

The possibility of imposing a charge for making information available in full or partial compliance with a request may dissuade the data subject from exercising his or her rights, and therefore should not be provided for in the GDPR, except in the cases already envisaged in Article 15(3) no. 2 and Article 12(5) no. 2 GDPR.

3. Brazil

The Brazilian Lei Geral de Proteção de Dados (LGPD) is a cross-sector regulation to protect personal data, which will enter into force in August 2020. Heretofore, the 'Marco Civil da Internet' has afforded data protection for specific data processing instances on the internet only. According to Article 18(2) LGPD, the data subject has a right to access to his or her data being processed, which represents a right to be informed about such data, while Article 18(5) LGPD grants a right to data portability.

Article 18 LGPD provides that

> The personal data subject has the right to obtain the following from the controller, regarding the data subject's data being processed by the controller, at any time and by means of request: […]
> II. *access* to the data; […]
> V. *portability* of the data to another service or product provider, by means of an express request and subject to commercial and industrial secrecy, pursuant to the regulation of the controlling agency; […].[25]

The LGPD is based on the GDPR, hence Article 18 LGDP largely corresponds to Articles 15 and 20 GDPR. The right to data portability is seen as one of the biggest innovations in Brazilian data protection law. The right applies to data being provided by the data subject and to generated data. Whether Article 20 GDPR has to be interpreted in the same way is subject to much discussion. The right to data portability is subject to commercial and industrial secrecy, which is also true for Article 20 GDPR. Article 20(4) GDPR even provides that the right to data portability may not adversely affect the rights and freedoms of other persons.

25 Emphasis added.

4. Japan

In Japan, The Act on the Protection of Personal Information (APPI) provides for cross-sector protection of personal data. Further data protection regulations can be enacted by each ministry for its specific area of competence, and the individual prefectures (federal states) make their own data protection law, some of which applies to the public sector only.

The APPI provides for a right to data access and the right to obtain a copy of the processed personal data under Article 28 APPI. The right to data portability is not provided for in Japan, but discussion of whether it should be introduced, especially with regard to the medical, finance and electricity sectors, is expected in 2020.

> Article 28 (Disclosure)
> (1) The person may request the business operator handling personal information to disclose the retained personal data that can be used to identify the person.
> (2) When the business operator handling personal information is requested under the provision of the preceding paragraph, the business operator must disclose the retained personal data without delay using the means that Cabinet Order provides for. However, in case falling under one of the following items, the business operator may choose not to disclose all or part of the retained personal data:
> (i) if disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party;
> (ii) if disclosure is likely to seriously interfere with the proper implementation of the business of the business operator handling personal information;
> (iii) if disclosure would violate any other law or regulation.
> (3) If a business operator handling personal information decides not to disclose all or part of the retained personal data as requested pursuant to the provision of the preceding paragraph (1), or there is no retained personal data, the business operator must notify the person of this without delay.
> (4) If, pursuant to the provisions of any other law and regulation, all or part of the retained personal data that can be used to identify a person is to be disclosed to the person by a means equivalent to what is prescribed in the main clause of paragraph (2), the provisions of paragraph (1) and (2) do not apply to either the whole or the relevant part of the retained personal data.

Article 28 APPI provides for a right of access to data as well as a right to obtain a copy, though the latter is not stated explicitly. The cabinet decides on the methods of disclosure but has not yet decided that access must be offered in an easy and precise way. No particular form is required, either. The request filed by the data subject also has to be precise. Exceptions of the duty to disclose data apply according to Article 28(2) APPI.

A crucial difference between the APPI and the GDPR is that under Article 33 APPI, disclosure of data can be made subject to payment of a fee. Apart from that, the provisions of the GDPR and the APPI are very similar.

5. India

Until recently, data protection obligations have only been imposed on companies, and have only been legislated in specific sectors (including telecommunications and finance) in India. These obligations are provided for in the Aadhaar (Targeted Delivery of Financial and other Subsidies Benefits and Services) Act, which dates from 2016. On 11 December 2019, India's Minister for Electronics and Information Technology introduced an updated draft of the Personal Data Protection Bill (PDPB) in the Lok Sabha, India's lower house of parliament. The Bill was referred to a Joint Select Committee consisting of parliamentarians from the lower and upper houses for examination and reporting.[26] The Committee is due to report back to the Lok Sabha by the second week of the 2020 monsoon session of parliament, which is about to run from September 14 to October 1.[27]

The new PDPB applies across sectors but to personal data only. General conditions for the exercise of the data subjects' rights are set forth in Section 21 PDPB, which mainly corresponds to Articles 13 and 14 GDPR.

---

26 Kurt Wimmer and Gabe Maldoff, 'India Proposes Updated Personal Data Protection Bill' (Inside Privacy 2019) <www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill> accessed 31 August 2020; Hunton Privacy Blog, 'India's Draft Data Privacy Bill Introduced in Parliament' (2019) <www.huntonprivacyblog.com/2019/12/19/indias-draft-data-privacy-bill-introduced-in-parliament> accessed 31 August 2020.

27 Surabhi Agarwal, 'Joint parliamentary committee wants more time to submit data bill note' (The Economic Times) <https://economictimes.indiatimes.com/tech/internet/jpc-wants-more-time-to-submit-data-bill-note/articleshow/74800912.cms> accessed 31 August 2020.

While Section 17 of the PDPB provides for a right to access to data, Section 19 PDPB introduces a right to data portability. Another right to customer data portability is currently in discussion for the insurance sector.[28] Whether it will actually be introduced is not yet clear. The PBPD partly uses misleading terminology. For example, it refers to the 'data principal' and not to the 'data subject' as other laws do, and to the 'data fiduciary' instead of the 'controller'. However, Section 3(13) and 3(14) clarify that there is no difference in meaning between 'data principal' and "data subject' or between 'data fiduciary' and 'controller'. According to Section 3(13), a 'data principal' is the natural person to whom the personal data relates. Section 3(14) provides that a 'data fiduciary' is any person, including the state or any company, juristic entity or individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

Sections 17 and 19 PDPB read as follows:

> Section 17 PDPB – Right to confirmation and access.
> (1) The data principal shall have the right to obtain from the data fiduciary—
> (a) confirmation whether the data fiduciary is processing or has processed
> personal data of the data principal;
> (b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof;
> (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7 in relation to such processing.
> (2) The data fiduciary shall *provide* the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.[29]
> (3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal

28 G. Naga Sridhar, 'Customer data portability to be introduced in insurance sector' (The Hindu Business Line 2018) <www.thehindubusinessline.com/money-and-banking/customer-data-portability-to-be-introduced-in-insurance-sector/article24584413.ece> accessed 31 August 2020.

29 Emphasis added.

data shared with them, in such manner as may be specified by regulations.

Section 19 PDPB – Right to data portability.
(1) Where the processing has been carried out through automated means, the data principal shall have the right to—
(a) *receive* the following personal data in a structured, commonly used and machine-readable format—
(i) the personal data provided to the data fiduciary;
(ii) the data which has been generated in the course of provision of services
or use of goods by the data fiduciary; or
(iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and
(b) have the personal data referred to in clause (a) *transferred* to any other data fiduciary in the format referred to in that clause.[30]
(2) The provisions of sub-section (1) shall not apply where—
(a) processing is necessary for functions of the State or in compliance of law or order of a court under section 12;
(b) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible.

Although the PDPB is based on the GDPR, there are some small differences. One of these is that Section 17 PDPB provides for data subjects' right to receive a summary of the data processing activities conducted. As under Brazilian data protection law, the right to data portability under Indian data protection law applies to data which is provided by the data subject, generated data, data which forms part of any profile of the data principal and data which the data fiduciary has obtained otherwise. It does not apply if processing is necessary for functions of the state or to comply with a law or court order. Nor does it apply if compliance with the request would reveal a trade secret of any data fiduciary, or is not technically feasible. The data fiduciary is not obliged to comply with requests under Sections 17 and 19 PDPB where such compliance infringes the rights of any other data principal under this Act, pursuant to Section 21(5) PDPB. According to Section 21(2) PDPB, the data fiduciary may charge a fee for complying with requests per Sections 17 and 19 PDPB, whereas this is only possible in exceptional cases under Article 12(5) GDPR.

30 Emphasis added.

6. Philippines

The Philippines Data Privacy Act (DPA), which dates from 2012, is a cross-sectoral regulation on personal data. Section 16 DPA grants the data subject a right of access to data, and a right to data portability is established in Section 18 DPA.

The relevant sections read as follows:

> Section 16. Rights of the Data Subject.
> The data subject is entitled to: […]
> (c) Reasonable *access* to, upon demand, the following:[31]
> (1) Contents of his or her personal information that were processed;
> (2) Sources from which personal information were obtained;
> (3) Names and addresses of recipients of the personal information;
> (4) Manner by which such data were processed;
> (5) Reasons for the disclosure of the personal information to recipients;
> (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
> (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
> (8) The designation, or name or identity and address of the personal information controller; […]
>
> Section 17. Transmissibility of Rights of the Data Subject.
> The lawful heirs and assigns of the data subject may invoke the rights of the data subject for which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.
> Section 18. Right to Data Portability.
> The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a *copy* of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to

31 Emphasis added.

> above, as well as the technical standards, modalities and procedures for their transfer.[32]
> Section 19. Non-Applicability.
> The immediately preceding sections are not applicable if the processed personal information is used only for the needs of scientific and statistical research and [...] for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

Apart from differences in details between Philippine data protection law and the GDPR, it is striking that under Section 17 DPA these rights are specifically transmissible, and may be invoked at any time after the death of the data subject, or when the data subject is incapacitated or rendered incapable of exercising the rights as enumerated in the immediately preceding section. Transmissibility is the subject of much discussion in relation to Article 20 GDPR.[33] The order of sequence of Section 17 DPA leaves ambiguity as to whether it refers only to Section 16 or to Section 18 as well. Since it concerns the rights of the data subject, it is to be assumed that despite its following after Section 16 it also refers to the right to data portability per Section 18 DPA.

Sections 16 and 18 are not applicable if the processed personal data are used only for scientific and statistical research, no activities are carried out on the basis of such nor decisions made regarding the data subject and the personal data are held under strict confidentiality and only used for the declared purpose. Nor are Sections 16 and 18 applicable to the processing of personal data gathered for investigation purposes regarding potential criminal, administrative or tax offences on the part of a data subject. Comparing the DPA with the GDPR, it is particularly striking that under the DPA data subjects' rights do not apply if the data is used for scientific research. Such an exception is missing in the GDPR. Although Article 89 GDPR provides that national law may allow exceptions to Article 15 for the purposes of scientific research and for exceptions to Article 20 if data is provided for public or archival purposes. Germany has not made use of this exception.

---

32 Emphasis added.

33 Jülicher and others (n. 11) 358, 360; Piltz (n. 11) 634; Strubel (n. 11) 356; Sperlich (n. 11) 377; Hennemann (n. 11) 6; Brüggemann (n. 11) 1; Herbst (n. 11) paras 1, 19; Kamlah (n. 11) Art. 20 DS-GVO paras 2–3; Rudolph (n. 11) Art. 20 DS-GVO para. 24; von Lewinski (n. 11) Art. 20 DSGVO paras 7, 113–114; Specht-Riemenschneider and Bienemann (n. 11) § 11 Rn. 7; Article 29 Working Party (n. 11) 3.

7. Singapore

The Singapore Personal Data Protection Act (PDPA) is a cross-sectoral regulation on personal data. Section 21 PDPA does not provide for a right to portability by law, but does grant data subjects a right of access to data. It is not applicable for the reasons listed in Section 21(2), (3) and (4).

Singapore is currently considering introducing data portability rights, as indicated by the government's latest discussion paper, but the country has not yet introduced such a right.[34]

> Access to personal data
> 21.
> (1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, *provide* the individual with —[35]
> (a) personal data about the individual that is in the possession or under the control of the organisation; and
> (b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.
> (2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.
> (3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to –
> (a) threaten the safety or physical or mental health of an individual other than the individual who made the request;
> (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
> (c) reveal personal data about another individual;
> (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

34 The Personal Data Protection Commission Singapore, 'Discussion Paper on Data Portability' (2019) <www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf> accessed 31 August 2020.

35 Emphasis added.

(e) be contrary to the national interest.
(4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant [...] or under any other written law.
(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4).

According to Section 21 PDPA and upon request, the data subject has a right to access the personal data used and to information on how the personal data has been or may have been used within the period of one year prior to the request date. The GDPR does not provide for such a temporal limitation. This right to access per Section 21 PDPA is subject to many exceptions. According to Section 21(2) PDPA, an organisation is not required to provide an individual with the individual's personal data or other information per subsection (1) in respect of the matters specified in the Fifth Schedule to the PDPA.[36]

Other reasons requiring compliance with Section 21(1) are stated in Subsection (3) PDPA. These include safety, health and privacy-related reasons, among others. In summary, Section 21 is subject to many more defined exceptions than is Article 15 GDPR.

36 The matters specified in the Fifth Schedule include opinion data, educational institutions, beneficiaries, private trusts, arbitral institutions and mediation centres, prosecution, protection of confidential commercial information and protection of trial, the prohibition of data processing by other special law, repetitious or systematic requests, unreasonable expenses, information that does not exist or cannot be found and trivial information (this can be compared to the purpose of protection per Art. 15(5) GDPR, which regulates that a request cannot be refused but that a fee may be charged). Thus Sec. 21(2) PDPA only offers a small opening clause for requests that are frivolous or vexatious, not a broad opening clause.

8. Switzerland

In Switzerland, the revised Data Protection Act is intended to replace the existing Swiss Federal Act on Data Protection (FADP). The FADP applies to personal data across sectors.

The revised version of the FADP provides for a right of access to data under Article 23, while a right to data portability is not provided for. However, a right to data portability is the subject of much current discussion. The Federal Council assumes that its introduction would be costly and its implementation difficult, which is why it has rejected a right to data portability.[37] Switzerland believes that not introducing such a right will not affect the attestation of equivalence within the meaning of the GDPR. The country thus favours sector-specific, voluntary agreements over a data portability right.

According to an expert from the University of Zurich, not having a right to data portability is not detrimental because companies could have the entitled person authorise them to exercise the right to information, thereby largely achieving the purposes of data portability via the current right to information.[38] It would be necessary however to amend the existing right to information in certain ways, and to exclude specific sectors which would be affected too negatively by such a right.[39]

Article 23 FADP (revised version) is scheduled to replace Article 8 FADP, and Article 24 FADP (revised version) will provide for exceptions to the right of access as provided for in Article 9 FADP today. Article 25 will provide for a right of refusal of information for the media, e.g. for the protection of informants as Article 10 FADP does currently. Articles 23, 24 and 25 essentially serve to implement Article 15 GDPR and contain only minor changes to the current legal situation. Information must be provided free of charge, but exceptions may be provided for by the Swiss Federal Council. Apart from details, Articles 8–10 FADP are very similar to the

37 Economie suisse, 'Gesetzliche Datenportabilität – kein Wundermittel' (2019) #05, 8 Dossier Politik <www.economiesuisse.ch/de/dossier-politik/gesetzliche-datenportabilitaet-kein-wundermittel> accessed 31 August 2020.

38 Rolf H. Weber and Florent Thouvenin, 'Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS)' (University of Zurich Center for Information Technology, Society, and Law 2017) <www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/datenpolitik/180321%20BJ-Gutachten_final.pdf.download.pdf/180321%20BJ-Gutachten_final.pdf> accessed 31 August 2020.

39 Ibid.

provisions of the GDPR. There are no significant advantages which need to be discussed here.

The current legal provisions read as follows:

> Article 8 – Right to information
> (1) Any person may request information from the controller of a data file as to whether data concerning them is being processed.
> (2) The controller of a data file must notify the data subject:
> a. of all available data concerning the subject in the data file, including the available information on the source of the data;
> b. the purpose of and if applicable the legal basis for the processing as well as the categories of the personal data processed, the other parties involved with the file and the data recipient.
> (3) The controller of a data file may arrange for data on the health of the data subject to be communicated by a doctor designated by the subject.
> (4) If the controller of a data file has personal data processed by a third party, the controller remains under an obligation to provide information. The third party is under an obligation to provide information if he does not disclose the identity of the controller or if the controller is not domiciled in Switzerland.
> (5) The information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge. The Federal Council regulates exceptions.
> (6) No one may waive the right to information in advance.
> Article 9 – Limitation of the duty to provide information
> (1) The controller of a data file may refuse, restrict or defer the provision of information where:
> a. a formal enactment so provides;
> b. this is required to protect the overriding interests of third parties.
> (2) A federal body may further refuse, restrict or defer the provision of information where:
> a. this is required to protect overriding public interests, and in particular the internal or external security of the Confederation;
> b. the information would jeopardise the outcome of a criminal investigation or any other investigation proceedings.
> (3) As soon as the reason for refusing, restricting or deferring the provision of information ceases to apply, the federal body must provide the information unless this is impossible or only possible with disproportionate inconvenience or expense.

(4) The private controller of a data file may further refuse, restrict or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties.
(5) The controller of a data file must indicate the reason why he has refused, restricted or deferred access to information.
Article 10 – Limitations of the right to information for journalists
(1) The controller of a data file that is used exclusively for publication in the edited section of a periodically published medium may refuse to provide information, limit the information or defer its provision provided:
a. the personal data reveals the sources of the information;
b. access to the drafts of publications would have to be given;
c. the freedom of the public to form its opinion would be prejudiced.
(2) Journalists may also refuse restrict or defer information if the data file is being used exclusively as a personal work aid.

III. Sector specific cross-type of data regulation

On 1 August 2019, Australia amended the Consumer and Competition Act (CCA)[40]2010 by introducing the so-called Consumer Data Right (CDR)[41] which is the basis for a sector-specific but cross-data type regulation. The CDR regime intends to give consumers extensive access to "their" data and should lead to a growth in (consumer) welfare.[42] For the purpose of such consumer welfare the CDR grants the consumer, among others, a right to data portability.[43] The purpose of Art. 20 GDPR, on the contrary, [44] is

40 Treasury Laws Amendment (Consumer Data Right) Bill 2019 (*As passed by both houses*) <https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6370_aspassed/toc_pdf/19126b01.pdf;fileType=application%2Fpdf> accessed 15 January 2020.

41 Consumer and Competition Act 2010 < https://www.legislation.gov.au/Details/C2017C00369> accessed 15 January 2020.

42 Explanatory Memorandum to Treasury Laws Amendment (Consumer Data Right) Bill 2019, part 1.3 et sey. <https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6370_ems_ce513d68-7222-49f4-a2fe-67e1c2b32fed/upload_pdf/712911.pdf;fileType=application%2Fpdf> accessed 15 January 2021.

43 Only a right is granted, but no corresponding, judicially enforceable claim. Judicial enforcement takes place at most indirectly through so-called civil penalties.

44 In addition to the portability right under the CDR, there is a cross-sectoral right of access comparable to that under Art. 15 GDPR. This is set out in the twelfth Australian Privacy Principle of the Privacy Act 1988 and relates to the storage and

mainly to address a data protection-related market failure in data markets.[45]

The CDR regime must be declared applicable to a specific sector and the legislator needs to work out specific regulations for that sector before they apply. Hence, the CDR regime can be described as a horizontal guideline for the legislator which gives orientation for specific regulation in certain sectors. Such specific regulation has yet only been implemented in the banking sector. Moreover, similar regulation is being prepared for the energy sector, and will follow for the telecommunications sector. [46]

According to Section 56AA CCA the object of the CDR is:

> (a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently:
> (i) to themselves for use as they see fit; or
> (ii) to accredited persons for use subject to privacy safeguards; and
> (b) to enable any person to efficiently and conveniently access information in those sectors that:
> (i) is about goods (such as products) or services; and
> (ii) does not relate to any identifiable, or reasonably identifiable, consumers; and
> (c) as a result of paragraphs (a) and (b), to create more choice and competition, or to otherwise promote the public interest.

1. CDR Data

Data (classes) which fall under the CDR regime can only be data that the legislature explicitly addresses or data which can be derived from such explicitly addressed data. CDR data can be both consumer and product related data.

---

control of personal information. Privacy Act 1988 <https://www.legislation.gov.au/Details/C2014C00076> accessed 15 January 2021.

45 Heike Schweitzer and Martin Peitz, `Data markets in the digital economy: functional deficits and regulatory needs' (2017) Discussion Paper No.17-043, 50 < http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf> accessed 15 January 2021.

46 For an overview of the implementation status <www.accc.gov.au/focus-areas/consumer-data-right-cdr-0> accessed 15 January 2021.

> Section 56AI Meanings of CDR data, directly or indirectly derived and CDR consumer
> CDR data is information that:
> (a) is within a class of information specified, as described in paragraph 56AC(2)(a), in an instrument designating a sector under subsection 56AC(2); or
> (b) is not covered by paragraph (a) of this subsection, but is wholly or partly derived from information covered by:
> (i) paragraph (a) of this subsection; or
> (ii) a previous application of this paragraph.
> (2) CDR data is directly or indirectly derived from other CDR data if the first-mentioned CDR data is wholly or partly derived from the other CDR data after one or more applications of paragraph (1)(b).
> (3) A person is a CDR consumer for CDR data if:
> (a) the CDR data relates to the person because:
> (i) of the supply of a good or service to the person or to one or more of the person's associates (within the meaning of section 318 of the Income Tax Assessment Act 1936); or
> (ii) of circumstances of a kind prescribed by the regulations; and
> […]
> (c) the person is identifiable, or reasonably identifiable, from:
> (i) the CDR data; or
> (ii) other information held by the other person referred to in paragraph (b); and
> […]

a) Consumer Data

Unlike the GDPR, the CDR does not intend to protect the informational self-determination but the data itself. Hence, legal entities can also be holders of the CDR data portability right if consumers have transferred the exercise of this right to them. However, whether data concerns the consumer and the consumer can therefore exercise or transfer the CDR rights depends on the identifiability of the consumer derived from European data protection law, see also 1.102 et seq. of the Explanatory Memorandum.

Speaking of derived data and the question whether the CDR rights apply to such derived data it needs to be pointed out that the meaning of 'derived data' in the GDPR differs from the meaning in the CDR regime. While the GDPR speaks of derived data as data being derived from data which has been entered by the data subject, the CDR regime means data

being derived from the data which was explicitly addressed in the sector specific regulation by the legislature, see subsection 56BD(1) Note 1 CCA. The CDR rights do not apply to derived data in the latter sense but data being derived from data which the data subject has entered could be explicitly addressed in the sector specific regulation and therefore the CDR data rights could apply to derived data in this sense.

Whether and to what extent a fee can be charged for the disclosure of data or for their subsequent use depends on whether the legislator has declared the data (classes) as being subject to a fee.

The relevant sections for the CDR consumer rights read as follows:

> 56BC Rules about disclosure, collection, use, accuracy, storage, security or deletion of CDR data for which there are CDR consumers
> *Required disclosures in response to valid requests*
> (1) Without limiting paragraph 56BB(a), the consumer data rules may include the following rules:
> (a) requirements on a CDR participant for CDR data to disclose all or part of the CDR data, in response to a valid request by a CDR consumer for the CDR data, to:
> (i) the CDR consumer for use as the CDR consumer sees fit; or
> (ii) an accredited person for use subject to the privacy safeguards; (...)
>
> 56BD Limitations for rules about CDR data for which there are CDR consumers
> *Only designated CDR data can be required to be disclosed*
> […]
> *No fee when fee-free CDR data is required to be disclosed*
> (2) The consumer data rules cannot allow a fee to be charged for:
> (a) the disclosure of fee-free CDR data under rules like those described in paragraph 56BC(1)(a) or 56BG(1)(a); or
> (b) the use of fee-free CDR data received as the result of such a disclosure.
> […]

b) Product Data

Product data, in contrast, is data that does not relate to any particular identifiable consumer. It includes information about terms and conditions, eligibility criteria, product pricing and so on. A product data request may be for required product data, voluntary product data or both. Subsection 56BF CCA identifies the data which needs to be disclosed upon request.

While a fee cannot be charged for the disclosure of required product data, a fee can be charged for disclosing voluntary product data. Under European law, in business-consumer relations product information must be provided in accordance with certain EU directives. These include directives on consumer rights and the distance marketing of consumer financial services, the provisions of which are implemented in the national law of the Member States (such as Articles 246 et seq. of the Introductory Act to the Civil Code, EGBGB, and Sections 312 et seq. of the Civil Code, BGB, in Germany). These information obligations apply without regard to a request filed by the consumer. It is therefore unnecessary to introduce a data access right to product data.

The relevant sections for product data in the CDR regime read as follows:

> 56BE Rules about disclosure, collection, use, accuracy, storage, security or deletion of product data
> Without limiting paragraph 56BB(b), the consumer data rules may include the following rules for CDR data for which there are no CDR consumers:
> (a) requirements on a CDR participant for the CDR data to disclose all or part of the CDR data to a person in response to a valid request by the person;
> [...]
>
> 56BF Limitations for rules about product data
> *Only certain kinds of product data can be required to be disclosed*
> (1) The consumer data rules can only require a disclosure of CDR data for which there are no CDR consumers if:
> (a) the CDR data is about the eligibility criteria, terms and conditions, price, availability or performance of:
> (i) a product or other kind of good; or
> (ii) a service; and
> (b) in the case where the CDR data is about availability or performance-the CDR data is publicly available.
> *No fee when this CDR data is required to be disclosed*
> (2) The consumer data rules cannot allow a fee to be charged for:
> (a) the disclosure of CDR data under rules like those described in paragraph 56BE(a) or 56BG(2)(a); or
> (b) the use of CDR data received as the result of such a disclosure.
> […]

2. *A hybrid approach to Data Governance*

The CDR regime does not only grant data access rights, but also determines the cornerstones of data governance, especially regarding the handling of these access rights. For example, a central body, the Data Standards Chair, should define technical standards for data transmission, which will then be binding. Such standards could also help to make Article 20 GDPR more effective.[47] Special attention should be paid to other actors described in the CDR regime who can and/or must be involved in handling data access:

a) Accredited persons

A difference between CDR and Article 20 GDPR is the possibility under the former that accredited persons may file consumer data requests on behalf of a consumer. In such situations the accredited person is authorized to receive or access the data directly. To be allowed to do so, the accredited person must pass a certification process , which means that several accreditation requirements must be met. These accreditation requirements may vary depending on the risk associated with the access to the data, i.e. in particular the type and manner of access and the sensitivity of the data in question – see 1.176 of the Explanatory Memorandum. In the banking sector, only one level of accreditation is provided for so far, which sets high standards for accreditation (for instance, an accredited person must take specific steps which relate to protecting CDR data from misuse, interference and loss - see subsection 5.2.3 of the Competition and Consumer (Consumer Data Right) Rules 2020).[48]

The GDPR does not provide for such a possibility for accredited person to receive or access data directly without the request of the data subject. Especially where markets are characterised by data-induced lock-ins, such a right could be helpful. By way of setting high standards for accreditation

47 See also Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation' COM(2020) 264 final, 10 et seq.

48 See also the further discussion: Consultation Paper 'CDR rules expansion amendments' (2020) <www.accc.gov.au/system/files/CDR%20rules%20expansion%20amendments%20-%20consultation%20paper%20-%2030%20September%202020.pdf> accessed 15 January 2021.

the risk for the data subject in terms of a possible loss of control over their data could be minimized. Such high standards could even raise the level of data protection (market-based approach to data privacy).

b) Gateways

Gateways are intended to enable more efficient and secure data transfer where necessary – see 1.95 and 1.180 of the Explanatory Memorandum. According to subsection 56BG(1), gateways can be intermediaries, i.e. a mediating authority for the purpose of data access. According to the CDR regime they could have different tasks, which could be specified as follows: Gateways can (i) manage data access and transfer by acting as an intermediary for the transmission of data and/or (ii) take over the management of access requests prior to data access. If possible, gateways should be under effective state control – see 1.97 of the Explanatory Memorandum. Such gateways under Australian law show certain parallels to the data intermediaries currently discussed in European law under the catchword 'data trustees'. The CDR regime could therefore also inspire European law in this respect

IV. Cross-sectoral and cross-type of data regulation

Even before the GDPR came into force, France had already implemented a very comprehensive data access and data portability right.[49] This covered both personal and non-personal data and applied to all data which a consumer placed online, which was otherwise generated or was in any way connected with his or her account. However, Article 48 of the Law for a Digital Republic was repealed in the course of the implementation of the GDPR. Today the French regulations correspond to those of the GDPR.

49 Art. 48 *Loi n° 2016–1321 du 7 octobre 2016 pour une République numérique* (Law for a Digital Republic), implementing such right as Arts. L 224–42–1 to L 224–42–3 *Code de consummation* (Consumer Law Code).

E. Findings and recommendations

The results can be summarised as follows:

1. Sector-specific regulation
   Sector-specific regulation mainly takes place in the telecommunications, energy, banking and mobility sectors. Occasionally there are also regulations for the health sector. These appear to be the most relevant sectors from a consumer perspective. However, further sectors may be added when a need arises. The advantage of sector-specific regulation is that the rights and interests of the actors concerned can be assessed much more accurately than under 'one size fits all' regulation. Sector-specific regulation thus affords more appropriate differentiation.
2. Cross-sector regulation
   The different legal systems which provide for data access rights across sectors but only regarding personal data essentially contain regulations that correspond, basically, to those of the GDPR. There are only a few differences concerning details, the most important of which are the following:
   a) Some jurisdictions provide that fees may be charged for granting access to personal data. This may prevent the data subject from exercising his or her rights, and is therefore not recommended.
   b) In some jurisdictions, the right to information is limited to data processing operations during a certain period, e.g. the previous 12-month period. This also falls short of the provisions of the GDPR, and is in any case not advisable from the perspective of the data subject.
   c) The same applies to rules requiring only a summary of the data processed to be given to the data subject.
   d) Some jurisdictions provide for more detailed lists of reasons for exclusion of data access rights than the GDPR entails. This creates more legal certainty than an open-ended general clause such as Article 15(4) GDPR, but affords less case-by-case justice.
   e) California, as well as Brazil, India and Australia, has legislated data portability rights with regard to generated data. If this were to be clarified in Article 20 GDPR, legislators could look to those jurisdictions as models.
   f) Some jurisdictions provide for an exception to data subjects' rights regarding data processing for scientific purposes. Such a regulation would be possible on the basis of Article 89 GDPR in national law, and could be needed in particular for medical research.

g) New Zealand permits the disclosure of personal data under terms and conditions. This is likely to mean restrictions on use of the data obtained. This might serve as an alternative to a refusal to provide personal data, also in the GDPR.

h) Some laws provide for the transferability of data subjects' rights. Apart from the USA (CPP), this concerns mainly the Philippines. Australia limits this possibility to accredited persons. Provided that high standards like those Australia has implemented for the accreditation process and that sanctions for data protection violations are in place, this would be a compromise that poses less of a threat to data subjects' interests than would be the case with full transferability.

i) The introduction of a right to non-discrimination for the exercising of data subjects' rights as in California's CCPA is highly recommended. The upholding of this right would essentially have to be monitored by data protection authorities, but consumer associations could be given the same powers they already have to prosecute other forms of discrimination.