IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-03

DATA PROTECTION BY DEFINITION

Report on the Law of Data Disclosure in Japan

Timo Hoffmann

March 2022

Place of Publication

University of Passau IRDG
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/

Author

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 deals with Japanese data law within the framework of a comparative study from legal studies, cultural studies and business informatics, which aims to investigate the extent to which decisions to disclose personal data are based on a cultural imprint as well as on the existing legal framework. To establish this, the country report sets a baseline. In addition to a brief overview of the Japanese legal framework, it deals decisively and in depth with issues relating to data law. The focus is on regulatory aspects relating to the collection, processing and dissemination of personal data. Central feature is the Act on the Protection of Personal Information (APPI), which covers the processing of personal data and establishes fundamental privacy rights for data subjects. Questions asked include: Which legal sources regulate Japanese data law? What are personal data in Japanese data law? How may these data be collected, processed and compliance enforced?

Cite as

Hoffmann, Timo. (2022). Data Protection by Definition– Report on the Law of Data Disclosure in Japan. *University of Passau IRDG Research Paper Series No. 22-03*. Available at https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Data Protection, privacy, Japan, Act on the Protection of Personal Information, data subject, processing, personal data, consent, business operator.

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.

Japan is a highly developed island nation in eastern Asia with a population of 124 million and home to one of the largest economies of the world.[1] The usage of data is valued as a possibility for economic growth,[2] but privacy and data protection were, at least until recently, not prominent issues.[3] Historically, privacy was recognized by the Japanese courts as a fundamental right, also allowing for civil litigation,[4] but a comprehensive law on data protection was, for a long time, absent. Japan's first comprehensive[5] law on the matter, the Act on the Protection of Personal Information (APPI)[6] was enacted in 2003.[7] It deals with the handling of personal information in general, with a focus on private businesses.[8] It is flanked by the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO)[9] and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (APPIHIAA),[10] which apply to the public sector in particular.

Despite introducing modern regulation on data privacy, it was comparatively weak in obligations, lacked its own regulatory agency, and drew criticism for enforcement perceived as lackluster.[11] This was mirrored by relatively low levels of concern by individuals on data protection issues.[12]

---

* 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 author would like to thank Dr. Frederike Zufall for her helpful comments that contributed to this report, Professor Dr. Moritz Hennemann for his support and guidance in the process, and André Rico Pacheco for his assistance.

[1] Central Intelligence Agency, 'Japan - The World Factbook' (4 February 2022) <https://www.cia.gov/the-world-factbook/countries/japan/> accessed 11 February 2022.

[2] Flora Y Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' [2020] Harvard Journal of Law & Technology 661, 661–662 <https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf> accessed 10 January 2022.

[3] For the development in the 2000s, see Andrew A Adams, Kiyoshi Murata and Yohko Orito, 'The Development of Japanese Data Protection' (2010) 2(2) Policy and Internet 93; For the internal Japanese developments preceding the adequacy decision, see Hiroshi Miyashita, 'EU-Japan Mutual Adequacy Decision' Blog Droit Européen <https://blogdroiteuropeen.files.wordpress.com/2020/06/miyashita-redo.pdf> accessed 11 February 2022.

[4] See *infra* Section C III 4 a.

[5] Earlier regulation on data protection existed as early as 1988 for the public sector, with court decisions on the topic from as early as 1964. See H. Miyashita, 'The evolving concept of data privacy in Japanese law' (2011) 1(4) International Data Privacy Law 229

[6] Available in English in the versions currently in force and set to come into force on 1 April 2022 at Personal Information Protection Commission, 'Laws and Policies' <https://www.ppc.go.jp/en/legal/> accessed 11 February 2022.

[7] Adams, Murata and Orito (n 3).

[8] See the overview at Personal Information Protection Commission, 'Current Legal Framework of the Protection of Personal Information' <https://www.ppc.go.jp/files/pdf/280222_Current_Legal_Framework_v2.pdf> accessed 2 February 2022.

[9] Available in English at <https://www.cas.go.jp/jp/seisaku/hourei/data/APPIHAO.pdf> accessed 11 February 2022.

[10] Available in English at <https://www.kobe-u.ac.jp/documents/en/about_us/rules/Act_on_the_Protection_of_Personal_Information_Held_by_Incorporated_Administrative_Agencies.pdf> accessed 11 February 2022.

[11] Graham Greenleaf, 'Japan—The Illusion of Protection' in Graham W Greenleaf (ed), *Asian data privacy laws: Trade and human rights perspectives* (1. ed. Oxford Univ. Press 2014); Adams, Murata and Orito (n 3).

[12] Yohko Orito and Kiyoshi Murata, 'Privacy Protection in Japan: Cultural Influence on the Universal Value' [2005] Proceedings of ETHICOMP

Significant change came with the commencement of trade talks between Japan and the EU preceding the enactment of the latter's GDPR,[13] with the Japanese government desiring to enable the free flow of data in order to benefit the economy.[14] As a result of this and through negotiation with the EU, Japan sought to obtain an adequacy decision under Art. 45 GDPR, allowing personal data from the EU to flow to Japan without the heavy restrictions on data transfers to non-EU member states. This required Japan to demonstrate its level of data protection is "essentially equivalent" to the level in the EU, i.e. comparable to the GDPR.[15]

As part of this development, Japan completely overhauled the APPI in 2015, with it coming into force on 30 May 2017, establishing the Personal Information Protection Commission (PPC) and guaranteeing data subject rights.[16] However, this alone was not enough to obtain the coveted adequacy decision. Reluctant to fully bring the APPI to the level of restrictions imposed on those processing personal data under the GDPR, "Supplementary Rules" were agreed on as part of the adequacy decision, which created stricter rules for personal information/personal data originating from the EU when processed in Japan, essentially creating a two-tiered system of data protection rules. To note is that the adequacy decision was reciprocal, as the APPI has a similar instrument: the EU is thus considered a region with an adequate level of data protection under Japanese Law. Altogether, one should note that the development of data protection legislation in Japan is less of an internal development than one necessitated by the EU's regulatory soft power, frequently called the "Brussels effect" and visible in a multitude of countries.

After the APPI's implementation, 2020 brought further changes – the APPI was again amended (as part of a Japanese mode of regulatory review of laws after a certain period of time) and toughened overall,[17] likely also with the EU's 2021 review of the adequacy decision[18] in mind. These amendments are set to come into force on 1 April 2022.[19]

The following report analyses Japanese law with regard to acts of disclosure of individuals' personal data, with a strong focus on the APPI as the central regulatory instrument.

<http://www.isc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf>; For a conceptual overview of privacy attitudes in Japan, see Makoto Nakada and Takanori Tamura, 'Japanese Conceptions of Privacy: An Intercultural Perspective' (2005) 7(1) Ethics Inf Technol 27 <https://link.springer.com/article/10.1007/s10676-005-0453-1> accessed 24 February 2022.

[13] Shizuo Fujiwara, Christian Geminn and Alexander Roßnagel, 'Angemessenes Datenschutzniveau in Japan - Der Angemessenheitsbeschluss der Kommission und seine Folgen' 2019 Zeitschrift für Datenschutz 204.

[14] Consider Shinzo Abe's speech, Prime Minister of Japan, 'Toward a New Era of "Hope-Driven Economy": The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting' (23 January 2019) <https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html> accessed 11 February 2022; Paul M Schwartz, 'Global Data Privacy: The EU Way' [2019] NYU Law Review 772, 791–792 <https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf> accessed 10 January 2022.

[15] Christopher Kuner, 'Article 45' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *Commentary on the EU General Data Protection Regulation* (Oxford University Press 2020) 774–775.

[16] Graham Greenleaf, 'Questioning 'Adequacy' (Pt I) – Japan' [2017] University of New South Wales Law Research Series, 241 <http://classic.austlii.edu.au/au/journals/UNSWLRS/2018/1.html> accessed 24 February 2022.

[17] Fumiaki Matsuoka and others, 'Atsumi & Sakai Newsletter | Amendments to the Act on the Protection of Personal Information' (2021) 25 <https://www.aplawjapan.com/application/files/5816/3339/3524/Newsletter_AS_016.pdf> accessed 14 January 2022.

[18] European Commission, 'Joint statement on the first review of the EU-Japan mutual adequacy arrangement' (26 October 2021) 25 <https://ec.europa.eu/newsroom/just/items/724795/en> accessed 11 February 2022.

[19] Personal Information Protection Commission (n 6).

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.

Perhaps the most striking characteristic of the Japanese legal system is its high degree of reception of foreign law.[20] Since Japan's period of modernization starting in the mid to late 19th century, it has again and again incorporated elements of foreign law into its own system, notably French and German law in the realm of private law, and American elements in constitutional and public law,[21] with strong German elements in administrative law tracing back to Prussian influence.[22]

The current constitution of Japan dates back to 1946 in the postwar period during American occupation. As a result of American intervention in the constitutional drafting process, the constitution was greatly influenced by US legal thought, and in some ways resembles the US political system.[23] Within the modern Japanese constitutional system, the Diet (source), consisting of the House of Representatives and the House of Councillors are responsible for lawmaking as the Japanese legislature. The Prime Minister as the head of the executive is elected by the diet, in turn appointing the Ministers to form the cabinet. The Judiciary is headed by the Supreme Court of Japan, which acts as a constitutional court, final court of appeal and has the power of judicial review.[24]

The constitution of Japan is the highest-ranking source of law.[25] Beneath the constitution is a wide array of codified law enacted by the Diet, followed by cabinet orders and ministerial ordinances. There further exist regulations by local authorities.[26] Case law also plays a role despite the fact that the Japanese system relies mainly on codification.[27] Furthermore, guidelines issued by public authorities can be of importance in many situations – while they are, strictly speaking, not legally binding, they often take the role of de facto law.[28]

Important to consider when looking at Japanese Law is the very low quantity of litigation and adversarial action when compared to similar economies.[29] This is often attributed to Japanese attitudes towards conflict and preference to other, informal modes of conflict resolution.[30] However, there may also be other explanations for this, with some pointing at the exceptionally low number of attorneys[31] in comparison to the

[20] Frederike Zufall, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (2019) 5(1) European Data Protection Law Review 17 <https://doi.org/10.21552/edpl/2019/1/6> accessed 24 February 2022.

[21] Robert Walters, Leon Trakman and Bruno Zeller, 'Japan' in Robert J Walters, Leon E Trakman and Bruno Zeller (eds), *Data protection law: A comparative analysis of Asia-Pacific and european approaches : European Union, Singapore, Australia, India, Indonesia, Malaysia, Thailand, Japan* (Springer 2019).

[22] Frederike Zufall, *Planungsrecht im Vergleich* (Beiträge zum ausländischen und vergleichenden öffentlichen Recht Band 37, 1. Auflage, Nomos Verlagsgesellschaft 2015).

[23] Hiroshi Oda, *Japanese Law* (4th edn, Oxford University Press 2021) 18–20.

[24] Ibid 25.

[25] Art. 98 of the Constitution states "This Constitution shall be the supreme law of the nation and no law, ordinance, imperial rescript or other act of government, or part thereof, contrary to the provisions hereof, shall have legal force or validity." English translation available at <https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html> accessed 11 February 2022.

[26] Oda (n 23).

[27] Ibid 24–25.

[28] For a thorough analysis of the role of guidelines in Japanese law, see Wang (n 2), 675–678.

[29] Birgit Fenzel, 'Debating the Japanese Approach to Dispute Resolution' [2011] MaxPlanckResearch Science Magazine 84 <https://www.mpg.de/4379741/W006_Culture-Society_084-091.pdf> accessed 11 February 2022.

[30] Wang (n 2), 679–686.

[31] This number was sought to be increased by the introduction of US-style law schools in 2004. This has, however, not led to substantial change in the long run,

size of the country,[32] which might simply make the justice system less accessible.[33]

The classification of Japan as belonging to a certain legal sphere is contested.[34] While it is often grouped with the Germanic civil law tradition due to the historical influences of German law, particularly in the area of private law,[35] other scholars dispute this attribution, referring to the multitudes of international legal influences[36] and the strongly divergent implementation of legal concepts of foreign origin.[37]

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

While there is no overarching codification of "Information Law" as a category, there exists a significant body of laws relevant for informational issues.

On the constitutional level, Art. 13 of the Constitution[38] is particularly significant: It contains a multi-faceted right to "being respected as an individual"[39] and has been interpreted by the Supreme Court of Japan as containing a right to privacy.[40] Other constitutional provisions that can be considered relevant to information regulation are articles 19 (freedom of thought and conscience), 21 (freedom of expression, prohibition of censorship and secrecy of communication), and 23 (academic freedom).

Japan is party to a multitude of international treaties on intellectual property[41] and has, in

with many law schools now closing down. See Andrew R J Watson, 'Changes in Japanese Legal Education' (2016) 21(41) 1 1–54-1–54 <https://www.zjapanr.de/index.php/zjapanr/article/view/1034>

[32] Martin Kellner, 'Legal Education in Japan, Germany and the United States: Recent Developments and Future Perspectives' (2007) 12(23) Zeitschrift für Japanisches Recht 195–205 <https://www.zjapanr.de/index.php/zjapanr/article/view/247> accessed 24 February 2022.

[33] Waldemiro F Sorte, 'Does the Japanese inclination towards non-litigation hinder access to justice for minority groups?' (2014) 4(3) IJPLAP 221 <https://www.inderscienceonline.com/doi/abs/10.1504/IJPLAP.2014.063003> accessed 24 February 2022.

[34] For a detailed discussion, see Harald Baum, 'Rechtsdenken, Rechtssystem und Rechtswirklichkeit in Japan – Rechtsvergleichung mit Japan' (1996) 1(2) Zeitschrift für Japanisches Recht 86–109 <https://www.zjapanr.de/index.php/zjapanr/article/view/910> accessed 24 February 2022.

[35] See discussion Ibid; For an analysis of German influence on Japanese private law, see Zentaro Kitagawa, 'Introduction: The Identity of Japanese and German Civil Law' in Zentaro Kitagawa and Karl Riesenhuber (eds), *The Identity of German and Japanese Civil Law in Comparative Perspectives/ Die Identität des deutschen und des japanischen Zivilrechts in vergleichender Betrachtung* (de Gruyter Recht 2007).

[36] Zufall, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (n 20).

[37] In depth Tsuyoshi Kinoshita, 'Legal System and Legal Culture in Japan' (2001) 6(11) Zeitschrift für Japanisches Recht 7–36 <https://www.zjapanr.de/index.php/zjapanr/article/view/673> accessed 24 February 2022.

[38] Art. 13 of the Constitution: "All of the people shall be respected as individuals. Their right to life, liberty and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs." English translation from <https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html> accessed 11 February 2022.

[39] Shigenori Matsui, 'Fundamental Human Rights and 'Traditional Japanese Values': Constitutional Amendment and Vision of the Japanese Society' (2018) 13(1) Asian J Comp Law 59 <https://www.cambridge.org/core/journals/asian-journal-of-comparative-law/article/fundamental-human-rights-and-traditional-japanese-values-constitutional-amendment-and-vision-of-the-japanese-society/C3CD7177248931D96EE302F434257007> accessed 24 February 2022.

[40] See *infra* Section C II 1.

[41] See, *inter alia*, World Intellectual Property Organization, 'WIPO-Administered Treaties - Contracting Parties < Japan'

accordance with international standard, enacted laws for the protection of rights[42] such as patents,[43] utility models,[44] registered designs,[45] copyright,[46] and trademarks.[47] Unregistered rights can be protected under the Unfair Competition Prevention Act.[48]

Provisions on cybercrime[49] can be found in the Act on Prohibition on Unauthorized Computer Access[50] and in the Penal Code, which contains a number of Articles especially for cybercrime.[51]

Other laws[52] deal with secrecy: amongst these is Art. 4 (1) of the Telecommunications Business Act,[53] which regulates different forms of electronic communications, provides that "secrecy of communications must not be violated". The Whistleblower Protection Act[54] does, to some extent, the opposite, protecting employees from retaliation when exposing misconduct.

The Basic Act on Cybersecurity[55] lays forth Japan's policy on cybersecurity, structuring measures to be taken by different public authorities.[56] Similarly, the Basic Act on the

<https://wipolex.wipo.int/en/treaties/ShowResults?country_id=87C> accessed 11 February 2022.

[42] For an overview, see Hitomi Iwase, Yoko Kasai and Satoshi Yumura, 'Intellectual Property Rights in Japan: Overview' (1 November 2020) <https://uk.practicallaw.thomsonreuters.com/5-501-5659> accessed 4 February 2022.

[43] Patent Act (Act No. 121 of 1959), English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=42&vm=02&re=02&new=1> accessed 11 February 2022..

[44] Utility Model Act (Act No. 123 of 1959) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3694&vm=02&re=2&new=1> accessed 11 February 2022.

[45] Design Act (Act No. 125 of 1959) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3695&vm=02&re=2&new=1> accessed 11 February 2022.

[46] Copyright Act (Act No. 48 of 1970) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3969&vm=02&re=2&new=1> accessed 11 February 2022.

[47] Trademark Act (Act No. 127 of 1959) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3696&vm=02&re=2&new=1> accessed 11 February 2022.

[48] Unfair Competition Prevention Act (Act No. 47 of 1993) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3629&vm=02&re=2&new=1> accessed 11 February 2022.

[49] Hiroyuki Tanaka, Daisuke Tsuta and Naoto Shimamura, 'Cybersecurity Comparative Guide' (13 August 2020) <https://www.mondaq.com/technology/976226/cybersecurity-comparative-guide> accessed 11 February 2022.

[50] Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3933&vm=02&re=2&new=1> accessed 11 February.

[51] Art. 161-2 (Unauthorized Creation of Electronic or Magnetic Records), Art.'s 163-2 to 163-5 (Unauthorized Creation, Possession and Preparation relating to Payment Cards with Unauthorized Electronic or Magnetic Records), Art. 168-2 (Making of Electronic or Magnetic Records Containing Unauthorized Commands), Art. 234-2 (Obstruction of Business by Damaging a Computer), Art. 246-2 (Computer Fraud), Art. 258 (Damaging Documents for Government Use) and Art. 259 (Damaging Documents for Private Use). Translation as Ibid.

[52] Refer to *infra* Section C III 1 a.

[53] Telecommunications Business Act (Act No. 86 of 1984), English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3390&vm=02&re=02&new=1> accessed 11 February 2022.

[54] Whistleblower Protection Act (Act No. 122 of 2004) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3362&vm=02&re=2&new=1> accessed 11 February 2022.

[55] Basic Act on Cybersecurity (Act No. 104 of 2014) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3677&vm=02&re=2&new=1> accessed 11 February 2022.

[56] For more information, see Roberto Carapeto, 'The Japanese Basic Act on Cybersecurity and the historical development of the Japanese legal framework for cybersecurity' (2021) 2(1) Int Cybersecur Law Rev 65

Formation of an Advanced Information and Telecommunications Society[57] does so concerning the promotion of ICT technologies. Another policy-setting law is the more recent Basic Act on the Formation of a Digital Society,[58] enacted with the aim of improving digital governance in Japan, coinciding with the Act on the Establishment of the Digital Agency, responsible for the "formation of a digital society".[59]

Other specific laws include the Act on Electronic Signatures and Certification Business,[60] which allows for electronic signatures, and the Act on the Regulation of Transmission of Specified Electronic Mail,[61] an anti-spam law. Furthermore, there exist laws on the protection of personal information and personal data.[62]

II. Allocation of Informational Legal Positions

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

Informational legal positions exist in the form of various intellectual property provisions, i.e. patents or trademarks. As echoed in Art. 1 of the APPI, Japanese regulators view data through a commercial lens, emphasizing data as a commodity.[63] In the area of (personal) data, there exist certain subjective rights of the respective principal together with legal restrictions on use and transfer for the protection of the individual the data is about.[64] There is, however, no legal concept of "data ownership" making informational goods other than those protected through IP rights not a commodity comparable to physical goods. Data "ownership" thus exists only as a de facto position.[65] A step towards protection of data as a commercial good comparable to intellectual property provisions was taken with the inclusion of protections for big data in the Unfair Competition Prevention Act in the 2018 amendment, whereby Art. 2 (7) sets forth a definition of "protected data", protecting holders of such data from improper acquisition.[66]

<https://link.springer.com/article/10.1365/s43439-021-00019-6#citeas> accessed 24 February 2022.

[57] Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (Act No. 144 of 2000) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3339&vm=02&re=2&new=1> accessed 11 February 2022.

[58] Digital Agency, 'Outline of the Basic Act on the Formation of a Digital Society' <https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_en_01.pdf> accessed 11 February 2022.

[59] Digital Agency, 'Outline of the Act on the Establishment of the Digital Agency' <https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_en_02.pdf> accessed 11 February 2022.

[60] Act on Electronic Signatures and Certification Business (Act No. 102 of 2000) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3821&vm=04&re=2&new=1> accessed 11 February 2022.

[61] Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002) English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3767&vm=02&re=2&new=1> accessed 11 February 2022.

[62] See *infra* Section C I.

[63] Wang (n 2), 669–670.

[64] See *infra* Section C III for a comprehensive overview of restrictions and rights relating to personal information/data.

[65] Atsushi Okada, 'Japan's legal approach to data transactions - SOLAIR Conference 2020' (10 September 2020) <https://solairconference.com/data/files/Japan-legal-approach-to-data-transactions.pptx>

[66] Yuriko Sagara, 'Big Data Protection under Unfair Competition Prevention Act has just started in Japan' (2019) <https://www.nakapat.gr.jp/ja/legal_updates_eng/big-data-protection-under-unfair-competition-prevention-act-has-just-started-in-japan/> accessed 11 February 2022.

III. Institutions

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

There are several government institutions and authorities relevant to the regulation of information and data related topics. These include the Cyber Security Strategy Headquarters and the National Information Security Center (NISC), tasked with dealing with cybersecurity issues,[67] the Personal Information Protection Commission (PPC),[68] the Japan Fair Trade Commission (source), Japan's competition law and antitrust regulator.

The Japan Patent Office (JPO)[69] is responsible for the registration of intellectual property rights such as patents, trademarks and registered designs, while the Agency of Cultural Affairs and the Software Information Center (SOFTIC) allow for registration of copyrights.[70] The Consumer Affairs Agency can be relevant for information law in the context of regulation of online consumer transactions. [71] The Public Security Intelligence Agency (PSIA) is responsible for surveillance of individuals and organizations deemed threatening.[72]

The Ministry of Internal Affairs and Communications is responsible for a wide range of topics concerning ICT infrastructure.[73] To this end, there exist authorities under its umbrella such as the National Institute of Information and Communications Technology (NICT), responsible for research and development of such technologies[74].

The perhaps most notable institutional development regarding information regulation in recent times, however, is the 2021 establishment of the Digital Agency.[75] It was created as a response to criticism in Japan's handling of the Covid-19 pandemic and is tasked with improving the digital capabilities of Japanese government institutions.[76]

Internationally, Japan is a member of international organizations such as the UN,[77]

---

[67] NISC, 'National center of Incident readiness and Strategy for Cybersecurity | About NISC' (1 February 2022) <https://www.nisc.go.jp/eng/index.html#sec1> accessed 3 February 2022.

[68] Personal Information Protection Commission, 'Roles and Responsibilities' <https://www.ppc.go.jp/en/aboutus/roles/> accessed 20 January 2022.

[69] Japan Patent Office, 'The Role of the Japan Patent Office' (13 August 2021) <https://www.jpo.go.jp/e/introduction/soshiki/yakuwari.html> accessed 3 February 2022.

[70] Iwase, Kasai and Yumura (n 42).

[71] Consumer Affairs Agency, 'Outline of the Consumer Affairs Agency' <https://www.caa.go.jp/en/about_us/> accessed 3 February 2022.

[72] Ministry of Justice of Japan, 'PSIA' (15 September 2021) <https://www.moj.go.jp/psia/English.html> accessed 3 February 2022.

[73] Ministry of Internal Affairs and Communications, 'Guidance on the Ministry of Internal Affairs and Communications' (21 February 2020) <https://www.soumu.go.jp/english/soumu/index.html> accessed 3 February 2022.

[74] NICT - National Institute of Information and Communications Technology, 'NICT - Home' (7 February 2022) <https://www.nict.go.jp/en/> accessed 7 February 2022.

[75] Digital Agency, 'Digital Agency' (2022) <https://www.digital.go.jp/en> accessed 3 February 2022.

[76] See Chitrali Parashar, 'Japan's Digital Agency: Another shot in the dark or an emblem of change' *Observational Research Foundation* (11 November 2021) 436 <https://www.orfonline.org/expert-speak/japans-digital-agency/> accessed 3 February 2022.

[77] United Nations, 'Member States' <https://www.un.org/en/about-us/member-states> accessed 3 February 2022.

the WTO,[78] the WIPO,[79] APEC[80] and the OECD.[81] It is also an observer of the Council of Europe's Convention 108.[82]

In the private sector, there exist numerous accredited personal information protection organizations tasked with establishing sectoral guidelines and assisting other organizations with the implementation of data protection procedures.[83] Concerning public informatory activity, there exists the NHK, Japan's public broadcasting organization.[84]

IV. Procedural Aspects

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

The Japanese enforcement system is characterized both by private enforcement through litigation[85] and administrative action.[86] Private litigation is generally possible through individual and a system of representative procedure, whereby individuals can group together claims, while stopping short of a class action system.[87]In the area of consumer protection, claims can also be brought by certain consumer organizations in the name of an indefinite group of consumers.[88] One should note, however, that, when compared to similar developed economies, significantly less litigation is brought before court,[89] mirrored by the similarly low number of attorneys per capita in Japan.[90] Even where action is brought, the majority of cases are settled in or out of court.[91]

Administrative authorities are, however, very present in Japan, though also not primarily through adversarial action, but strongly reliant on informal mechanisms such as guidance and advice. Appeals against administrative action are possible.[92] However, Japan does not have a specialized administrative court system as in other jurisdictions. Furthermore, there exist government-specific alternative dispute

---

[78] World Trade Organization, 'WTO Members and Observers' (13 August 2018) <https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm> accessed 3 February 2022.

[79] World Intellectual Property Organization, 'Information by Country: Japan' (8 December 2021) <https://www.wipo.int/members/en/details.jsp?country_id=87> accessed 3 February 2022.

[80] APEC, 'Member Economies' <https://www.apec.org/about-us/about-apec/member-economies> accessed 3 February 2022.

[81] OECD, 'About the OECD' (5 January 2022) <https://www.oecd.org/about/> accessed 3 February 2022.

[82] Council of Europe, 'Convention 108 in the World - Parties' (2022) <https://www.coe.int/en/web/data-protection/convention108/parties> accessed 2 February 2022.

[83] See *infra* Section C IV 2 b.

[84] Japan Broadcasting Corporation (NHK), 'NHK Corporate Information' (18 June 2021) <https://www.nhk.or.jp/corporateinfo/> accessed 3 February 2022.

[85] For a good overview, see Akihiro Hironaka, 'Litigation: Japan' (20 May 2021) <https://globalarbitrationreview.com/insight/know-how/litigation/report/japan> accessed 4 February 2022.

[86] See Michael Asimov, 'A Comparative Approach to Administrative Adjudication' in Peter Cane and others (eds), *The Oxford Handbook of Comparative Administrative Law* (Oxford University Press 2021) 588.

[87] Oda (n 23).

[88] Toshitaka Kudo, 'Group Litigation (Class Action) in Japan' in Keio Insitute for Global Law and Development (ed), *How Civil Law Is Taught in Asian Universities* (Programs for Asian Global Legal Professions Series. Keio University Press 2019).

[89] Giorgio F Colombo and Hiroshi Shimizu, 'Litigation or Litigiousness? Explaining Japan's "Litigation Bubble" (2006-2010)' [2016] Oxford University Comparative Law Forum <https://ouclf.law.ox.ac.uk/litigation-or-litigiousness-explaining-japans-litigation-bubble-2006-2010/> accessed 26 January 2022.

[90] Kellner (n 32); Watson (n 31).

[91] Oda (n 23) 444.

[92] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76, recitals 103-112.

resolution systems, particularly in consumer protection contexts.[93] In the context of information law, special courts exist regarding certain intellectual property rights.[94]

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

The main piece of legislation concerning data protection law in Japan is the Act on the Protection of Personal Information (APPI), originating from 2003. It was significantly amended multiple times, most notably in 2017. The most recent updates are from 2020, set to enter into force on 1 April 2022.

The APPI is the overarching framework for data protection law in Japan. Its general provisions are applicable to both private and public sector activity, while specific rules for the handling of personal information are applicable only to the private sector. Specific provisions for public entities are found in the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO) and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (APPIHIAA). Furthermore, there exist numerous regional regulations[95] on the handling of personal information by prefectures, cities, towns and villages.[96]

Supplementary to the APPI as the main source of law, there is the Cabinet Order,[97] the Basic Policy on the Protection of Personal Information[98] as well as a number of guidelines enacted by the PPC which go into more detail and are not merely advisory, but to be considered binding.[99] Additionally, there exist several data protection provisions in other laws, such as in Art. 5-4 of the Employment Security Act.[100] Outside of specific data protection law, there are civil remedies based on tort law that rely on the classification of privacy as a protected right under Art. 13 of the Japanese Constitution,[101] which are also very relevant in disputes concerning data protection.

Private sector regulation can be found in the form of sectorial (industry-specific) guidelines.[102] Lastly, as a consequence of the EU-Japan Adequacy Decision, there exist supplementary rules concerning the handling of personal information originating from the European Union,[103] which establish a two-tier system with relatively stricter requirements

---

[93] Keiko Okuhara, 'Researching Japanese Law - GlobaLex' (12.2020) Section 6.5 <https://www.nyulawglobal.org/globalex/Japan1.html> accessed 4 February 2022.

[94] Oda (n 23) 434.

[95] Toshihiro Wada, 'Data Protection in Japan' (Turning Point in Data Protection Law) 148.

[96] Providing a good overview: Personal Information Protection Commission, 'Current Legal Framework of the Protection of Personal Information' (n 8).

[97] Cabinet Order to Enforce the Act on the Protection of Personal Information, English translation available at <https://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf> accessed 2 February 2022.

[98] See Art. 7 APPI; Basic Policy on the Protection of Personal Information, available in Japanese at <https://www.ppc.go.jp/files/pdf/300612_personal_basicpolicy.pdf> accessed 2 February 2022.

[99] For the nature of guidelines in Japanese Law, see Wang (n 2), 674–678.

[100] Employment Security Act of 30 November 1947, last amended 2019, English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3645&vm=04&re=01&new=1> accessed 2 February 2022. See also Wada (n 95) 148.

[101] See *infra* Section C III 4.

[102] See Adequacy Decision, recital 73.

[103] Supplementary Rules, Adequacy Decision Annex 1.

for dealing with such EU personal information – however, some core differences were eliminated following the 2020 amendments[104] to the APPI,[105] bringing the rules for Japanese data closer to what is contained in the supplementary rules.

The APPI, the core piece of data protection legislation, is generally influenced by the EU's GDPR, which can be seen as a consequence of the political factors at play in its 2017 redrafting, which was done with the aim of obtaining an adequacy decision from the EU. Similar to the GDPR, for instance, is the partially exterritorial scope of application set forward in Art. 75, which requires handling of personal information of a person in Japan or in the context of providing such persons with goods and services. However, there exist some core differences: Notably, the APPI does not name "principles" of data/personal information protection. It also does not impose a general ban on processing subject to factors permitting processing of personal information. The central, overarching requirement is the specification of the purpose of handling of personal information.[106] Consent (or alternatives thereto) are not always needed, with much regulation hinging on further transfer of personal data/information rather than the initial point of collection.[107]

Regarding regulatory technique, the APPI is especially notable through its extensive use of different definitions of personal data or personal information, dependent on the degree of collation or structuring, sensitivity or de-identification and imposing nuanced obligations dependent on the nature of the personal information at hand[108] – while exposing the APPI to criticism that some of its requirements are not applicable to all that is worthy of protection.[109] This mode of regulation can be seen as risk-based.[110]

Art. 76 APPI rather broadly excludes several areas from the applicability of the APPI, these being the press, professional writers, universities and academia, and religious and political organizations, however only where using personal information for purposes specific to them, and with the *caveat* in paragraph (3), whereby these shall still "strive to take[111] (…) necessary and appropriate action for the security control of personal data".

Hidden in plain sight is another restriction of the scope of the APPI through the concept of the business operator:[112] Private individuals and organizations handling personal information for purposes other than business are thus not subject to the provisions of the APPI.

Important for a comprehensive understanding of the Japanese system is the collaborative or "cooperative" approach of the PPC[113] and Japanese Enforcement Agencies in General:[114] This report, in the following sections, goes into further depth on legal provisions relevant for acts of disclosure of personal data.

---

[104] Tomomi Fujikouge and Naoto Kosuge, 'Amendment of Japan's Act on the Protection of Personal Information' (4 August 2020) <https://www.dlapiper.com/en/japan/insights/publications/2020/08/amendment-of-japans-act/> accessed 14 January 2022.

[105] Most significantly, the definition of "retained personal data" was changed, making Supplementary Rule 2 redundant.

[106] See *infra* Section C III 2 b.

[107] See *infra* Section C III 1.

[108] See *infra* Section C II 1.

[109] Reference critical assessment of the definition of personal information in the APPI – there was an article on this.

[110] Reference SOURCE on the concept of risk-based regulation.

[111] This wording indicates non-enforceability of the provision, see *infra* Section C III 2 b (n 174).

[112] For definition, see *infra* Section C II 3.

[113] See especially Wang (n 2).

[114] See *supra* Section A II.

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. 13 of the Japanese Constitution of 1947[115] creates the right to be "respected as individuals" as well as rights to life, liberty and the pursuit of happiness.[116] In 1969, the Japanese Supreme Court,[117] in a decision concerning photographs taken of an individual by police, it recognized a right to "freedom in private life", giving "any person (…) the right not to have his face or appearance photographed without consent or good reason", thus establishing a right that might today be considered a right to privacy or data protection.[118] More recently, in 2008, the Japanese Supreme Court held that Art. 13 of the Constitution contains a right to privacy, stating that "every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or made public without good reason".[119]

The Act on the Protection of Personal Information (APPI) in its current version[120] contains many different concepts of personal data as well as related concepts, these being "personal information" (Art. 2 (1)), an "individual identification code" (Art. 2 (2)), "special care-required personal information" (Art. 2 (3)), a "personal information database etc." (Art. 2 (4)), "personal data" (Art. 2 (6)). "retained personal data" (Art. 2 (7)), "pseudonymously processed information" (Art. 2 (9)), "anonymously processed information" (Art. 2 (11)), and "personally referable information" (Art. 26-2 (1)). Further specification on these definitions can be found in the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order).[121] The APPI approach relies on these different categories and concepts of personal data[122] in order to incentivize[123] certain behaviors and provide rules adequate for the respective risks.[124]

---

115 Available in English at <https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html> accessed 1 February 2022.

116 Art. 13 of the 1947 Constitution of Japan: "All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs.", Ibid.

117 Courts in Japan, 'Supreme Court of Japan' (28 January 2022) <https://www.courts.go.jp/english/index.html> accessed 1 February 2022.

118 Supreme Court, Judgment of the Grand Bench of 24 December 1969, Case Number 1965 (A) 1187, Keishu Vol. 23, No. 12, at 1625. Available at <https://www.courts.go.jp/app/hanrei_en/detail?id=34>.; See also Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 6-9.

119 Supreme Court, Judgment of the First Petty Bench of 6 March 2008, Case Number 2007 (O) 403, Minshu Vol. 62, No. 3. Available at <https://www.courts.go.jp/app/hanrei_en/detail?id=1276> accessed 14 January 2022.

120 Amended Act on the Protection of Personal Information (Tentative Translation), Personal Information Protection Commission, Japan (June, 2020). Available in English at <https://www.ppc.go.jp/files/pdf/APPI_english.pdf> accessed 1 February 2022.

121 Cabinet Order available in English at <https://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf> accessed 14 January 2022.

122 See also the table in Taro Komukai, 'Data Protection in the Internet: Japanese National Report' in Dário Moura Vicente and Sofia de Vasconcelos Casimiro (eds), *Data Protection in the Internet* (vol 38. Springer International Publishing 2020) 257.

123 See for example the Adequacy Decision, recital 25, whereby the PPC stated that the 6-month period for the use of retained personal data exists to incentivise a short period of processing and retention.

124 Christian Geminn, Anne Laubach and Shizuo Fujiwara, '„Schutz anonymisierter Daten im

The central definition is "personal information" in Art. 2 (1) APPI. It "means information relating to a living individual" as part of two variants. Art. 2 (1) (i) names several examples, clarifying it encompasses "any and all matters (…) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (…) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual). The other variant in Art. 2 (1) (i) concerns such "information relating to a living individual (…) containing an individual identification code", which is then defined in Art. 2 (2) and specified in greater detail, listing different types of such codes, in Art. 1 of the Cabinet Order.

Based on the definition of "personal information" but narrower in scope is the definition of "personal data" in the APPI. "Personal data" is briefly defined as "personal information constituting a personal information database etc." in Art. 2 (6), the latter being defined in Art. 2 (5) which is "a collective body of information comprising personal information" requiring a degree of systematic organization and further specified in Art. 3 of the Cabinet Order.

Even more specific is the definition of "retained personal data" defined in Art. 2 (7) and Art. 4 and 5 of the Cabinet Order. Prior to the revision of the APPI in 2020,[125] this definition excluded data to be deleted within 6 months,[126] easing compliance requirements for such data – and prompting the adequacy decision by the EU to require, in Supplementary Rule 2,[127] that personal data transferred from the EU be considered such. With the revision, all personal data, except for those exempt under Art. 4 of the Cabinet Order, are now considered retained personal data, eliminating a key level of risk-oriented differentiation and lessening the significance of this definition in comparison to "normal" personal data.

From this structure, one can see that all "retained personal data" is "personal data" and all "personal data" is also "personal information", while the opposite, respectively, is not true.

Another feature of the 2020 overhaul of the APPI is the inclusion of the term "personally referable information" in Art. 26-2, which is even broader than "personal information": "information relating to a living individual which does not fall under personal information, pseudonymously processed information or anonymously processed information". It thus acts as a sort of catch-all provision surpassing even the few restrictions to the term of "personal information", and is intended for information where identification is difficult, as with cookies.[128]

A further differentiation is included is the definition of "special care-required personal information" in Art. 2 (3) APPI, a staple in international data protection laws, which includes such data considered especially sensitive and thus worthy of extra protection, e.g. medical data. The definition is further specified in Art. 2 of the Cabinet Order.

The definitions of "pseudonymously processed information" in Art. 2 (9) and "anonymously processed information" in

japanischen Datenschutzrecht – Kommentierung der neu eingeführten Kategorie der ‚Anonymously Processed Information'" [2018] Zeitschrift für Datenschutz.

[125] Fujikouge and Kosuge (n 104).

[126] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92); See also the prior Version, available in English at <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf> accessed 14 January 2022.

[127] Ibid.

[128] Matsuoka and others (n 17).

Art. 2 (11) deal with personal information de-identified to a certain degree in order to allow for less risk – corresponding with less onerous compliance obligations.

The Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (APPIHIAA) contains materially identical definitions of "personal information" in Art. 2 (2), an "individual identification code" in Art. 2 (3), and "special care-required personal information" and Art. 2 (4). The definition of "anonymized personal information" in Art. 2 (8) corresponds to the definition of "anonymously processed information". Similarly, the definition of "personal information file" in Art. 2 (6) corresponds to "personal information database etc." in the APPI. Differences can be found in the definition of "retained personal information" in Art. 2 (5), which (roughly) means such personal information recorded in documents by an incorporated administrative agency and does not hinge on the duration of retention, such as in the APPI.

The Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO) contains definitions of "personal information" in Art. 2 (2), which is similar, but more simplistic and without reference to an "individual identification code", when compared to the APPIHIAA and APPI. The definitions of "retained personal information", Art. 2 (3), and "personal information file", Art. 2 (4), correspond to the definitions of the APPIHIAA.

The My Number Act[129] incorporates definitions of the APPI, APPIHIAA and APPIHAO by reference. Its definition of "personal information" in Art. 2 (3) includes everything considered personal information by the other acts, while its definition of "personal information file" in Art. 2 (4) refers to the same term in the APPIHIAA and APPIHAO and to the term of "personal information database etc." in the APPI. Specific to the aim of the My Numbers Act, it then gives its own definitions for "individual number", Art. 2 (5), "specific personal information", Art. 2 (8), which does not correspond to the term of special care-required personal information (!), and, based on this, "specific personal information file" in Art. 2 (9).

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.

Within the APPI, the term referring to an individual person is "principal", as defined in Art. 2 (8): "A "principal" in relation to personal information in this Act means a specific individual identifiable by personal information". Thus, similarly as in other data protection legislation around the world, referentiality between data/information and the individual is by the data being "about" them.

In the APPIHAO, Art. 2(5) uses the terminology of the "Individual Concerned", whereas the APPIHIAA, in Art. 2(7) uses the term "relevant individual". These two Acts, however, refer to the individual as being "identified", rather than "identifiable".[130] The My Numbers Act simply speaks of a "person" in Art. 2 (6).

Differentiation between domestic and foreign nationals occurs indirectly,[131] through

[129] English translation available at <https://www.ppc.go.jp/files/pdf/en3.pdf> accessed 11 February 2022.

[130] Read in comparison the definition of "data subject" in Art. 4 (1) GDPR which highlights that data can be considered identifiable in contrast to identified.

[131] Graham Greenleaf, 'Japan: EU Adequacy Discounted' [2019] University of New South Wales

the two-track model[132] established by the supplementary rules as part of the EU-Japan Adequacy Decision[133] – however, these differentiations technically rely on the fact that the data is received from the EU, rather than the data being "about" EU citizens.

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.

In categorizing different types of parties handling personal data, the APPI speaks of different types of "business operators", similar to the European data controller,[134] mirroring the categories of personal data/personal information definitions.

These are the "personal information handling business operator" (PIHBO), in Art. 2 (5), the "pseudonymously processed information handling business operator" (PPIHBO) in Art. 2 (10), the "anonymously processed information handling business operator" (APIHBO) in Art. 2 (12) and the "personally referential information handling business operator" in Art. 26-2 (1) of the APPI. Therefore, the role of the recipient, and thus, his/her obligations, varies depending on the type of data or information processed.

The term business operator implies use of the data in business and therefore excludes public entities and recipients of data using the data for private, non-commercial purposes – however, with the reform of the APPI in 2017, size-based restrictions were abolished, meaning that now, companies are obliged to comply with the relevant rules irrespective of the amount of data processed.[135]

Differentiation between business operators occurs along the borders of persons/legal entities – this can be especially relevant when assessing whether a subsidiary of a Japanese company outside of Japan is considered a "third party in a foreign country" as in Art. 24 APPI,[136] which deals with the PIHBO's provision of data to such foreign third parties and limits outsourcing. Data obtained through merger or business succession is, in some cases, not considered to be obtained from a third party, Art. 23 (5) (ii) APPI – however, when the purpose of data usage changes, advance consent is still necessary, Art. 16 (2) APPI.

While the APPI does not explicitly acknowledge a concept of a "processor" as under the GDPR, it references "trustees" in Art. 22, also considered PIHBOs, obliging the entrusting PIHBO to supervise them.[137] The concept of an "accredited personal information protection organization" does not create a different legal situation concerning obligations to the processing of

Law Research Series <https://ssrn.com/abstract=3276016> accessed 13 January 2022.

[132] Term used by Wang (n 2), 665.

[133] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92).

[134] Walters, Trakman and Zeller (n 21) 249.

[135] Ulrich Kirchhoff and Tobias Schiebe, 'The Reform of the Japanese Act on Protection of Personal Information. From the Practitioner's Perspective' (2017) 22(44) 1 199–212, 200–201 <https://www.zjapanr.de/index.php/zjapanr/article/view/1178> accessed 24 February 2022.

[136] Noriko Higashizawa and Yuri Aihara, 'Data Privacy Protection of Personal Information Versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)' (2017) 84(4) Defense Counsel Journal, 9 <https://www.iadclaw.org/assets/1/19/Data_Privacy_Protection_of_Personal_Information_Versus_Usage_of_Big_Data.pdf?228> accessed 13 January 2022.

[137] Recital 35, Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92).

personal information for such organizations. These are rather to be understood as having an advisory and regulatory support role for business operators, see Articles 47-58 APPI.[138]

The public is not considered a recipient in a technical sense. However, in several situations, the public may be the addressee of transparency requirements. This is the case (as a variant next to informing the individual) in Art. 18 (1) and (3) APPI concerning the communication of the utilization purpose.[139] Moreover, Art. 27 APPI deals with the public disclosure of certain information concerning the handling of personal data.

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".

The term "disclosure" appears in the English translation of the APPI as the term for one of the principal's rights under Art. 28 (1). However, disclosure in the sense of an individual disclosing his/her own personal information to another party is not explicitly regulated. Nevertheless, there exist numerous provisions relevant for such acts of disclosure, most importantly in the APPI. While personal information is not considered a (commercial) good in the legal sense (notwithstanding the possibility of it being protected by other intellectual property provisions in parallel), the introductory Art. 1 APPI states that "the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society", implying that the commercial aspect of such acts of disclosure are important to Japanese regulators.[140]

The "data law" framework for such acts of disclosure of personal data consists mainly of the APPI, the APPIHAO, the APPIIAA and the accompanying regulations, as discussed above.[141] While a constitutional right to privacy exists under Japanese law, it was not developed through the term of "informational self-determination".[142] Details on the relevant provisions for data disclosure are discussed in the following sections.

a. Disclosure Prohibitions

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

Disclosure of personal data can be prohibited as a consequence of Art. 23 APPI for PIHBOs. Where the disclosing party is considered a PIHBO, they must obtain consent of those principals concerned by the personal data that is to be disclosed or be considered under the other variants mentioned in Art. 23 (1) APPI. However, as individuals would only considered a PIHBO when acting for business purposes, this would not generally prevent the disclosure of data referential to persons other than the discloser.

Confidentiality obligations can also arise as a consequence of privileged professions as well as from contractual agreements.[143] Additionally, trade secrets are protected under Art. 2 of the Japanese Unfair

[138] See also *infra* Section C IV 2 a and b.

[139] In the case of pseudonymously and anonymously processed information, disclosure to the public is the standard mode of fulfilling transparency requirements, Art. 35-2 (4) and (6), Art. 35-3 (2) and Art. 36 (3) and (6) APPI.

[140] See in comparison Wang (n 2), 670.

[141] See *supra* Section C I.

[142] See *supra* Section C II 1.

[143] Daisuke Morimoto and Toshihiko Hamano, 'Confidentiality Q&A: Japan' (2020) <https://uk.practicallaw.thomsonreuters.com/w-027-0037> accessed 13 January 2022.

Competition Prevention Act.[144]This Act was further revised to give confidentiality protections to "protected data" in Art. 2 (7), aiming to protect big data applications.[145]

A notable secrecy provision was introduced with the highly controversial[146] State Secrets Law from 2013.[147] It (criminally) prohibits the "handling" of "specially designated secrets".[148] This designation can be given to certain documents or records by administrative organs.

Furthermore, confidentiality provisions can be found for the telecommunications sector,[149] e.g. in the Telecommunications Business Act.

b. Disclosure Obligations

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

Japanese Law knows obligations to register residence and information relevant for family status with public registries under the Basic Resident Registration Act[150] and the Family Register Act,[151] thus creating obligations to provide authorities with individuals' personal information. Similarly, tax law can create obligations to provide personal information as part of the part of the process of filing tax returns.[152]

In this context, one can also mention the My Number Act, which introduced uniform individual identification numbers for individual to ease public administration[153] but has been criticized as problematic.[154]

Aside from the limited government powers to intercept communications,[155] to search and seizure of records, public authorities collect information through "enquiry sheets" without the possibility of enforcement. However, this may still, to a certain extent, compel individuals or companies (PIHBOs) to disclose their personal information, or, more problematic, that of others.[156]

---

144 English translation available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=3629&vm=02> accessed 13 January 2022.

145 Sagara (n 66).

146 Justin McCurry, 'Abe defends Japan's secrets law that could jail whistleblowers for 10 years' *The Guardian* (10 December 2014) <https://www.theguardian.com/world/2014/dec/10/japan-state-secrets-law-security-dissent> accessed 13 January 2022.

147 Act on the Protection of Specially Designated Secrets, Act. No. 108 of December 13, 2013. English translation available at < http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2543&re=02&vm=02> accessed 13 January 2022.

148 Marcelo Corrales, 'Right to Know v. the Secrecy Law in Japan: Striking the Right Balance' (2014) 19(38) Zeitschrift für Japanisches Recht 189–200 <https://www.zjapanr.de/index.php/zjapanr/article/view/413> accessed 24 February 2022.

149 Komukai (n 122) 254–255.

150 Basic Resident Registration Act 25 June 1967, available in English at <https://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/pdf/111026_1.pdf> accessed 27 January 2022.

151 Family Register Act 22 December 1947, available in English at <http://www.japaneselawtranslation.go.jp/law/detail/?id=2161&vm=02&re=02&new=1> accessed 27 January 2022.

152 Marcus Wong and Ichiro Kawakami, 'Japan - Individual - Tax administration' (16 August 2021) <https://taxsummaries.pwc.com/japan/individual/tax-administration> accessed 27 January 2022.

153 Komukai (n 122).

154 See on this topic Yohko Orito, Kiyoshi Murata and Chung A Young, 'E-Governance Risk in Japan: Exacerbation of Disciriminative Structure Built in the Family Registration System' in Terrell Ward Bynum and others (eds), *ETHICOMP 2013 Conference Proceedings: The possibilities of ethical ICT* (2013).

155 Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 121-124.

156 Ibid. Recitals 125-129.

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).

The Japan Fair Trade Commission, in 2019, published the new "Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.".[157] As of these Guidelines, the JFTC considers abuses of a superior bargaining position, defined in this case as "when the consumers, even though suffering detrimental treatment from the digital platform operator, is compelled to accept this treatment in order to use the services provided by the digital platform operator",[158] as an abuse of a superior bargaining position under Art. 2 (9) (v) of the Antimonopoly Act,[159] thereby protecting consumers in this unequal context.[160]

Concerning employees, data protection law does not provide for special rules addressing the unequal relationship to the employer to protect their voluntariness. However, there exist guidelines of the Ministry of Health, Labour, and Welfare and the Ministry of Economy, Trade, and Industry concerning the practice of monitoring employees.[161]

Additionally, there are no specific provisions regarding minors or children.[162]

As is the case in many data protection laws worldwide, requiring consent of affected persons for certain acts of processing or usage of data features frequently and prominently in the APPI:

Art. 16 (1) requires PIHBOs to obtain advance consent from principals when handling personal information "beyond the necessary scope to achieve a utilization purpose",[163] referring to the required specification of purpose in Art. 15. Additionally, Art. 16 (2) requires advance consent in order to continue using data in accordance with the specified utilization purpose in case of company succession or merger. Art. 16 (3) sets out exceptions to these two paragraphs, e.g. when "based on laws and regulations" (i) and the protection of "human life, body or fortune" (ii).

The acquisition of special care-required personal information, in general, always requires a principal's advance consent as of Art. 17 (2), also subject to exceptions in the items named under Art. 17 (2). Advance consent is also required when providing personal *data*[164] to a third party as of Art. 23 (1), and, combined with stricter information requirements, when providing personal data to a third party in a foreign country, Art. 24 (1).

---

157 Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc. 17 December 2019. English translation available at <https://www.jftc.go.jp/en/legislation_gls/imonopoly_guidelines_files/191217DPconsumerGL.pdf> accessed 14 January 2022.

158 Ibid 4–5.

159 Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Act No. 54 of April 14, 1947) 1947. Available in English at <https://www.jftc.go.jp/en/policy_enforcement/21041301.pdf> accessed 14 January 2022.

160 Saori Hanada, Fumiaki Matsuoka and Osamu Fujiwara, 'The top three data protection law topics in Japan: Data Protection | Spring 2020 | Legal Briefing' (2020) <https://www.inhouselawyer.co.uk/legal-briefing/the-top-three-data-protection-law-topics-in-japan/> accessed 14 January 2022.

161 Komukai (n 122) 260.

162 Ibid 259.

163 Note that this only includes changes of purpose and does not require consent for the initial act of processing in compliance with the primary utilization purpose.

164 Note that personal *data* is narrower in scope compared to personal *information*, see Section C II 1.

Concerning personally referable information,[165] Art. 26-2 also requires consent[166] be given by the principal[167] when such information is transferred to a third party or a third party in a foreign country and when "it is assumed that a third party will acquire personally referable information (…) as personal data".

The APPI itself, however, does not give more detail as to specific prerequisites for such consent, and especially does not provide a definition.[168] There exist, however, certain guidelines as soft law instruments that give more guidance.[169]

2. Recipient Obligations

a. Requirements for Personal Data Reception

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

Starting point for regulation in the APPI is the "handling" of personal information/personal data. While this term is not defined in the APPI itself or in PPC guidelines, it is understood broadly, and similarly to the broad definition of processing in Art. 4 (2) GDPR, encompasses collection, retention, use, transfer and other acts.[170] As such, reception of relevant information or data would be considered "handling".[171]

Following this categorization and when looking at obligations relevant in the stage of or prior to reception, the recipient needs to comply with the relevant APPI obligation. Always relevant in this stage is the specification of an explicit utilization purpose, Art. 15. The PIHBO is required to fulfil information requirements regarding the utilization purpose as put forward in Art. 18 (1) – this can be done by disclosing the utilization purpose to the public in advance, or by "promptly" afterwards informing the principal or the public. In case of pseudonymously processed information, Art. 35-2 (4) specifies that the correct mode is disclosure to the public, only. Art. 18 (2) names situations where a notification of the public is not sufficient.

Specific to the reception phase is Art. 17 (1), stating generally the prohibition of acquiring "personal information by deceit or other improper means", and Art. 17 (2), which requires advance consent when *acquiring* special care-required personal information,[172] though only alternative to presence of one of the cases enumerated in items (i) to (vi).[173]

Indirect requirements for reception can arise when acquiring personal data not from the principal, but from another PIHBO. In this case, the other (providing) PIHBO will in some cases need to obtain consent under Art.

---

[165] See Section C II 1.

[166] Note, however, that Art. 26-2 does not specify the consent be in advance, as opposed to the other provisions discussed above.

[167] The use of the term *principal* here is somewhat peculiar, as the definition relates to *personal data*, not *personally referable information*. An explanation could be the prerequisite of the data to be acquired *as personal* data. See Section C II 2.

[168] Compare this to the detailed definition of consent in Art. 4 (11) GDPR.

[169] See the information given in Walters, Trakman and Zeller (n 21) 258–259.

[170] See also Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 17.

[171] Daniel Hounslow and Ryuichi Nozaki, 'Japan - Data Protection Overview' (2021) <https://www.dataguidance.com/notes/japan-data-protection-overview> accessed 14 January 2022.

[172] As opposed to Art. 16 (1) and (2), which are linked to "handling" the data. Art. 16 (1) is not especially relevant to the phase of reception since (simple) reception beyond the specified utilization purpose is difficult to imagine when pursuing another specified utilization purpose, since acquisition of the personal information is necessary in any case. This could be different, however, when the PIHBO fails to specify *any* utilization purpose.

[173] Item (vi) allows for acquisition without consent where prescribed by a cabinet order, which could, at least in theory, be exploited by government to hollow out the general consent requirement.

23 or Art. 24,[174] The receiving PIHBO is required to "confirm" the contact information of the providing PIHBO and the "circumstances under which the said personal data was acquired" under Art. 26 (1) (i) and (ii), or, in the case of personally referable information, Art. 26-2 (1) (i) and (ii).

Informatory requirements not linked to an individual act of reception are contained in Art. 27, concerning retained personal information.[175] These refer to information such as a corporate address or contact information, utilization purposes and information on principals' rights.[176]

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.

The central obligation concerning handling of personal information is the observance of the utilization purpose,[177] which must be specified, Art. 15 (1), and my not be altered beyond "the scope reasonably relevant to the pre-altered utilization purpose", Art. 15 (2) APPI. Handling of personal information beyond this scope requires advance consent as of Art. 16 (1) and is thus inadmissible without such consent, except where items (i) to (iv) of Art. 16 (3) apply.[178] Altering the utilization purpose also requires notification of the principal or public disclosure, Art. 18 (3) APPI.

Art. 19 APPI requires the PIHBO to keep personal data[179] "accurate and up to date within the scope necessary to achieve a utilization purpose", and to "delete the personal data without delay when such utilization has become unnecessary". Art. 20 APPI contains a general obligation for the PIHBO for security of personal data, in order to prevent "leakage, loss or damage", complemented by duties to supervise employees, Art. 21, and entrusted persons/trustees, Art. 22. Notification requirements in case of leakage are contained in Art. 22-2 APPI.[180] Specific security obligations also exist to prevent re-identification of pseudonymous or anonymous data, see Art. 35-2 (2), Art. 36 (2), Art. 36 (6) and Art. 39 APPI. Remarkable is that even organizations exempt from the majority of APPI provisions[181] are required to "strive[182] to take (…) necessary and appropriate action" concerning security, Art. 76 (3) APPI. Security provisions going into more detail are contained in PPC guidelines.[183]

Next to the obligation to delete personal data when the utilization purpose is fulfilled, the concept of "retained personal data", Art. 2 (7) previously incentivized using personal data for only a short period, as some obligations only came forth when retaining data for a

---

[174] This would be the case where the receiving party is considered foreign – which is possible due to the broad scope of applicability as set forth by Art. 75 APPI.

[175] Note that, since the 2020 changes to the APPI, the term *retained personal data* is largely equivalent to *personal data*. See Section C II 1.

[176] See *infra* Section C III 3 a.

[177] Internationally, this concept is termed "purpose limitation", see e.g. Art. 1 (b) GDPR.

[178] These being "cases based on laws and regulations" (i), "cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent" (ii), enhancement of public hygiene and for the promotion of children's health (iii) and certain cases of government cooperation (iv).

[179] For definition, see *supra* Section C II 1.

[180] See *infra* Section C IV 1 b.

[181] Exempt from the obligations of Chapter IV.

[182] The wording "strive" implies the non-enforceability of this individual provision. See also footnote 59 of the Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), which calls this a "best effort" obligation.

[183] Ibid, recitals 57-59.

period longer than six months. With the 2020 revision of the APPI, such an additional incentive no longer exists.[184]

Concerning further transmission of received personal data, Art. 23 deals with such provision to third parties in general, with Art. 24 putting forth additional rules for international transfers. In Art. 23, there are two general variants for provision of personal data to a third party. The first is contained in Art. 23 (1) and allows for such transfer on the basis of consent or on the basis of items (i) to (iv). The second variant, in Art. 23 (2), allows for transfer without consent (and the other items) but has additional prerequisites: In this case, certain information must be provided to the principal,[185] and they must be given the right to opt out of the transfer.[186] Special care-required personal information may, however, only be transferred on the basis of Art. 23 (1), and thus, in general, only with consent of the principal.

Exceptions and specifications are contained in Art. 23 (3) to (6). When a PIHBO acquires personal information from another PIHBO, it is possible to set a new utilization purpose – on this basis, the adequacy decision implements a special rule for data originating from the EU, obligating the PIHBO to "confirm the specific purpose(s) underlying the transfer … and further process the data in line with such purposes".[187]

Art. 24 APPI goes further in prohibiting, in general, the transfer of personal data outside of Japan without consent. Countries recognized as having "equivalent standards" to Japan concerning personal information protection are not considered a "foreign country". Art. 24 also does not apply where a PIHBO has taken the necessary action to protect individuals' personal data, called "equivalent action", Art. 24 (3) APPI. The EU adequacy decision, in Supplementary Rule (4), requires that consent be "particularly well informed".[188] As part of the 2020 amendments to the APPI,[189] the PIHBO is, under the amended version, required to provide additional detailed information on personal information protection in the foreign country, Art. 24 (2).

Art. 26-2 APPI contains specific requirements for the transfer of personally referable information if "it is assumed that a third party will acquire personally referable information (…) as personal data", thus increasing protection.

3. Discloser Control

a. Transparency and Entitlement to Information

Central to the transparency requirements in the APPI[190] is the obligation under Art. 18 (1) APPI, whereby the PIHBO must inform data subjects of the utilization purpose, which can be done individually towards the principal/data subject or through advance disclosure "to the public", and must also be done in case of an allowed change of purpose under Art. 18 (3).

Concerning retained personal data,[191] Art. 27 APPI names general requirements for transparency, stating the PIHBO shall "put

---

[184] See *supra* Section C II 1.

[185] "Informed a principal of those matters set forth in the following or put them into a state where a principal can easily know".

[186] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 47.

[187] Ibid, recital 49; Supplementary Rule (3).

[188] Ibid, recital 76; Supplementary Rule (4).

[189] Fujikouge and Kosuge (n 104).

[190] See also "Transparency" in Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 60-64.

[191] See *supra* Section C II 1.

those matters forth in the following into a state where a principal can know" – thus stopping short of individual (active) notification. In practice, this is done via privacy policies.[192] This includes information such as address and name of the PIHBO (i), the utilization purposes of all such data (ii), and on the procedure concerning the use of the individual rights under Articles 28-30 APPI. There exist some (limited exceptions to this).[193]

Further specific information requirements exist for transfers to third parties under Art. 23 and 24 APPI. Information of the principal is a central requirement for transferring data to third parties under the variant of Art. 23 (2) with the possibility of opting out rather than through consent, with items (i) to (viii) listing contents of such information.[194] Art. 24 (2) APPI, since the 2020 revision,[195] requires "information on the personal information protection system of the foreign country, on the action the third party takes for the protection of personal information, and other information that is to serve as reference to the principal".

b. Co-Determination and Co-Decision Concerning Date 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.

While certain acts under the APPI require advance consent,[196] data subject, or in the terminology of the APPI, principal co-determination is significantly weaker after data has been collected by the PIHBO, due to the fact that the APPI does not provide for the revocation of consent given.[197]

The main principal rights are contained in Art. 28, 29 and 30 APPI.[198] Art. 28 is the right to "disclosure" of retained personal data,[199] which must be provided in the form of an "electromagnetic record", or in case of this being an excessive burden, in a written document, Art. 28 (2). This is subject to exceptions under items (i) to (iii) of Art. 28 (2), such as "cases of violating other laws or regulations". The PIHBO responsible must also inform a principal in case of noncompliance with the request, Art. 28 (3).

Art. 29 gives the principal the right of "correction etc.", allowing them to request "correction, addition or deletion" where contents of retained personal data "are not factual". This does therefore not equal a general right to deletion. The PIHBO is required to inform the principal of action taken or not taken as a consequence, Art. 29 (3).

Art. 30 (1) gives the principal the right to demand a "utilization cease etc.", which means the PIHBO must either delete or stop using the retained personal data. This right is limited, however, to situations where the retained personal data is handled in violation of Articles 16 and 16-2, which concern the proper setting of a utilization purpose, or was

---

[192] Hiroyuki Tanaka and Noboru Kitayama, 'Japan enacts Amendments to the Act on the Protection of Personal Information' (2020) <https://iapp.org/news/a/japan-enacts-the-act-on-the-protection-of-personal-information/> accessed 20 January 2022.

[193] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 64.

[194] See *supra* previous section.

[195] Fujikouge and Kosuge (n 104).

[196] See *supra* Section C III 1 c on matters requiring such advance consent.

[197] Walters, Trakman and Zeller (n 21) 250 state this "is considered as being a major gap in Japan's laws".

[198] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 81-94.

[199] Note that this is not applicable to all personal information.

acquired in violation of Art. 17, i.e. through "deceit or improper means" or, concerning special care-required personal information, without consent.[200] As such, this right is also tied to a previous illegal situation, rather than creating an overarching right.

Where a PIHBO transfers personal data to a third party under Art. 23 (2), a right to opt out of the transfer is created for the principal ("where it is set to cease in response to a (…) request a third party-provision of personal data").

c. Revocation

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

There is no right to data portability in japan – however, the right to "disclosure" in an "electromagnetic record" is at least partially similar, albeit not leading to an end to processing. As discussed in the previous section, there is no right to deletion or revocation of consent in the APPI – aside from the obligation to "strive to (…) delete the personal data when (…) utilization has become unnecessary" in Art. 19, to which provision there is no corresponding right, with Art. 30 not naming Art. 19 as grounds for demanding a utilization cease. As such, ex post deletion is not at all prominent in the APPI, and, as can be argued, in Japanese data protection law in general.

This can be seen in the Japanese discussion on the topic of the "right to be forgotten", which takes place in the context of an individual wishing not to be listed in online search results and engaged in a civil suit against a search engine provider. The existence of such a right was confirmed by the Japanese Supreme Court in 2017,[201] despite deciding against the plaintiff in the case, and is based on the personality right in Art. 13 of the Japanese Constitution.[202] However, such a right, logically building on the right to privacy, only exists in balance to a societal "right to know", following the right to freedom of expression as based on Art. 21 of the Japanese Constitution.[203] The "right to be forgotten" is thus limited.[204]

d. Procedural Aspects

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

Articles 31 to 35 of the APPI contain provisions concerning the procedure for PIHBOs to follow when complying with and responding to requests under the APPI individual rights in Articles 28 to 30.

Art. 31 states the PIHBO must explain the reason for acting or not acting upon such requests. Article 32 (1) gives the PIHBO the right to decide on a method for receiving requests (in accordance with the cabinet order, which, in Article 10, states the areas to be decided on as being where and how to file the demand (i), the format of document to be submitted (ii), methods for confirming the identity of principal or agent (iii), and the method for fee collection (iv). Such collection of fees is allowed as of Art. 33, but it may only be "within a range recognized as reasonable considering actual expenses". The PIHBO may demand the principal to "present a matter sufficient to specify retained personal data", Art. 32 (2). Art. 32 (3) states the principal may make demands via an agent Art. 11 of the Cabinet Order clarifies this can

---

[200] Or one of the items listed in Art. 17 (2) APPI, see Section C III 2 a.

[201] Supreme Court, Decision of the Third Petty Bench of 31 January 2017, Case Number 2016 (Kyo) 45, Minshu Vol. 71, No. 1. Available at <https://www.courts.go.jp/app/hanrei_en/detail?id=1511> accessed 18 January 2022.

[202] See Walters, Trakman and Zeller (n 21) 253–254. This may be enforced by means of a civil suit based on Art. 709 of the Japanese Civil Code. See also *infra* Section C III 4 a.

[203] For an in-depth analysis, see Zufall, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (n 20).

[204] Ibid.

be either a statutory agent, (i) or an agent entrusted by the principal, (ii).

Article 32 (4) prohibits the PIHBO from imposing an excessive burden on the principal, with Art. 35 (1) obliging the PIHBO to "strive to deal appropriately and promptly with a complaint about the handling of personal information". For this, Art. 35 (2) states, the PIHBO "shall strive to establish a system necessary to achieve" this, thus making it a responsibility to appropriately organize to allow for handling of demands.

Art. 34 APPI requires principals to allow for passage of two weeks after making a demand before filing a lawsuit in this regard, thereby giving PIHBOs the right to react.

4. Enforcement

a. Damages and Compensation

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

While the APPI itself does not provide for the awarding of damages or other compensation of individuals in case of violations of data protection law, damages can be claimed through Art. 709 of the Japanese Civil Code,[205] which deals with tort claims in general. This requires the affected individual to sue the offending party[206] on the basis they have "intentionally or negligently infringed any right of others, or legally protected interest of others".[207] Compensation for mental or psychological harm can be obtained under Art. 710, with liability for employees provided by Art. 715.[208] The right or legally protected interest of others, as required by the provision,[209] can be any protective article of the APPI (or other data protection laws) as well as the more general rights arising from Art. 13 of the Japanese Constitution.[210]

Compensation is *compensation*, with punitive damages absent from Japanese law.[211] Non-pecuniary loss is compensated as of Art. 710 on a case-by-case basis.[212] As quantification of harm or damages in cases of privacy or data protection infringement is rather difficult, significant uncertainty exists concerning actual amounts of compensation to be expected.[213]

It should be noted that, in several cases and in adherence to social expectations, companies have voluntarily provided victims of data breaches with compensation in the form of coupons.[214]

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".

As the existence of Art. 34 APPI and the aforementioned Art. 709 of the Japanese Civil Code suggest, action can be brought before

---

[205] See, in comparison to German law, Julian Hinz, 'Das Recht der Mediation im japanisch-deutschen Vergleich' (2019) 24(47) Zeitschrift für Japanisches Recht 143–178 <https://www.zjapanr.de/index.php/zjapanr/article/view/1344> accessed 24 February 2022.

[206] Wang (n 2), 675.

[207] Translation by Japan Ministry of Justice, 'Japanese Law Translation - [Law text] - Civil Code' (2009) <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2057&re=02&vm=02> accessed 12 January 2022.

[208] See Komukai (n 122) 264–266.

[209] Referring to the broad interpretation of this Oda (n 23) 196–197.

[210] See Section C II 1.

[211] Béligh Elbati, 'The Supreme Court of Japan on Punitive Damages…' (2021) <https://conflictoflaws.net/2021/the-supreme-court-of-japan-on-punitive-damages/> accessed 12 January 2022.

[212] Oda (n 23) 202.

[213] Walters, Trakman and Zeller (n 21); See table detailing compensation in several court cases in Komukai (n 122) 265.

[214] Detailing this feature of the Japanese legal context Wang (n 2), 680.

Japanese courts via standard civil procedure.[215] A basic requirement of such action is standing, meaning that the claimant must "have a legitimate interest in the subject matter of litigation".[216] In accordance with the civil law tradition, Japan does not know different standards of proof, but rather gives the judge presiding over the case a large amount of discretion.[217] In this context, the low degree of litigiousness in Japan should be mentioned – even where disputes go to court, many cases are settled.[218] Aside from litigation, there exist arbitration, used mostly in commercial contexts, and mediation,[219] most commonly conducted in family disputes.[220] These are therefore not particularly relevant in the context of data protection/privacy.

IV. Objective Legal Obligations of the Recipient

1. Duties Concerning Received Data

a. Dependence on Authorization

Of business models, processing variants, terms and conditions.

Administrative authorization is not a common feature in the APPI, and processing/handling itself is subject to the various legal provisions, not to such authorization.

Articles 47 to 58, however, contain provisions for the accreditation of certain organizations as "accredited personal information protection organizations" subject to several requirements aiming at establishing a proper standard for dealing with personal information protection by assisting PIHBOs.[221] This accreditation gives the organizations some enforcement rights, such as the right to request action from business operators under Art. 52 (3) APPI, which the business operator may not request without a justifiable reason.

b. Notification Duties

Of business models and business activity; of processing activity.

There are no general notification or registration requirement under the APPI. A relevant notification obligation vis-à-vis the PPC exists where onward transfers of data occur on the basis of the opt-out-mechanism, Art. 23 (2) APPI.[222]

Notification duties further exist in the form of obligations to report on data breaches, as contained in Art. 22-2 APPI, an innovation of the 2020 amendments to the APPI. It includes the obligation of PIHBOs to report to the PPC "when there is a leakage, loss or damage (…) and it is prescribed by the rule of the Personal Information Protection Commission as those of which there is a large possibility of harming an individual's rights and interests." This refers to the Amendment rules of the PPC, which clarifies the types of leakage necessitating such a report.[223]

---

[215] See also Section A II.

[216] Oda (n 23) 435.

[217] For more detail, see Kevin Clermont, 'Standards of Proof in Japan and the United States' (2004) 37(2) Cornell International Law Journal 263, 265 <https://scholarship.law.cornell.edu/cilj/vol37/iss2/1> accessed 24 February 2022.

[218] Oda (n 23) 444.

[219] Hinz (n 205).

[220] Chie Yakura and Yuka Teraguchi, 'Litigation and Enforcement in Japan: Overview' (2021) <https://uk.practicallaw.thomsonreuters.com/9-502-0319> accessed 24 February 2022.

[221] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 73-74.

[222] Akemi Suzuki, 'Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Japan' (27 October 2021) <https://uk.practicallaw.thomsonreuters.com/w-026-4239> accessed 3 February 2022.

[223] Matsuoka and others (n 17) 8, containing an English translation of the provision.

It should be noted, however, that, even before the amendments, reporting to the PPC in case of problems or when needing guidance was commonplace[224] and a feature of the climate of collaboration present within Japan concerning regulatory authorities.[225]

c. Documentation

Accountability.

Explicit documentation requirements to ensure accountability[226] are contained in Articles 25 and 26 of the APPI. These deal with record-keeping regarding transfers of personal data from one PIHBO to another, Article 25 from the perspective of the transferor, Article 26 that of the transferee. Articles 12 to 18 of the PPC Rules contain further specification, especially on which information exactly shall be recorded and on the methods of recording. The general time period for keeping of records is 3 years, Art. 25 (2) and Art. 26 (4) APPI, specified in Art. 14 and Art. 18 PPC Rules, respectively. Art. 26 (1) (ii) APPI requires the receiving PIHBO to confirm the "circumstances under which the said personal data was acquired by the said third party", and, according to Art. 15 (2) PPC rules, the disclosing PIHBO must provide the receiving PIHBO with documentation supporting this.

This is modified concerning personal data originating from the EU by Supplementary Rule 3, which requires the receiving PIHBO to keep a record of "the fact that the data originates from the European Union as well as the purpose of the original data transfer".[227]

It is notable that, under the system of the APPI, such documentation is explicitly required only for transfers of personal data between PIHBOs, not when a PIHBO collects such data merely for use by itself. However, an indirect obligation to keep records on retained personal data can be considered to exist as a consequence of the obligation to properly comply with other provisions of the APPI, especially under Art. 35 (2) APPI, which requires the PIHBO to "strive to establish a system" for compliance with the principal's individual rights vis-à-vis the PIHBO. In order to do this, a PIHBO will factually need to record certain information necessary for such actions as verifying the identity of the concerned principal.

Lastly, documentation is also provided via the annual reports of the accredited personal information protection organizations.[228]

d. Processing Requirements

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

The APPI does not use the (GDPR) regulatory model of pre-emptively banning processing, or "handling", in the Japanese terminology, of personal information/data. Thus, there exists no general prohibition subject to permission. Handling of personal information is allowed in principle, with the APPI provisions to be followed, first and foremost the specification of the utilization purpose in Art. 15. Terms and conditions law is contained in Articles 548-2 to 548-4 of the Japanese Civil Code, but is not as strongly developed as elsewhere.[229] It could nevertheless be relevant for contexts where

[224] Ibid 2.

[225] Considering this the main feature of Japanese data protection law Wang (n 2).

[226] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 70-74.

[227] Ibid, recital 71.

[228] Ibid, recitals 73-74.

[229] Jürgen Basedow, 'AGB-Kontrolle in Japan und Deutschland' (2020) 25(49) Zeitschrift für Japanisches Recht 187–200 <https://www.zjapanr.de/index.php/zjapanr/article/view/1452> accessed 24 February 2022.

the mode of handling personal data or personal information is specified in consumer contracts.

The only mention of a "contract" in the APPI is in Art. 18 (2), stating that the utilization purpose for the personal information must be stated explicitly in the contractual document, thus linking contracts concerning individuals with informatory requirements.

2. Monitoring

a. Recipient Self-Monitoring

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

As noted above,[230] the PIHBO is bound to "strive to establish a system necessary" (Art. 35 (2)) to "deal appropriately and promptly with a complaint about the handling of personal information" (Art 35 (1)), aiming primarily at effectively guaranteeing compliance with the principals' rights under Articles 28 to 30 APPI. The APPI, however, does not contain explicit requirements regarding the structuring of such an internal system. In contrast to several other international data protection laws,[231] there is no strict legal requirement for the appointment of data protection officers. However, such an obligation can arise in order to be compliant with guidelines.[232]

To a certain extent, self-monitoring occurs via the documentation requirements.[233]

Accredited personal information protection organizations can also assist PIHBOs in dealing with matters of personal information protection, as set out in the items of Art. 47 APPI, these then considered "covered" by the accredited organizations, Art. 51 APPI, especially concerning dealing with complaints, Art. 52 APPI.

b. Regulated Self-Regulation

Industry associations.

The APPI establishes a framework for voluntary self-regulation by industry, as is reflected in Art. 53 APPI and linked to the accredited personal information protection organizations. These organizations shall "strive to develop a guideline conformable to the purport of the provisions of this act". The guidelines are then sent to the PPC and published, Art. 53 (2) and (3). After the act of publishing, the accredited personal information protection organization then, through "guidance or recommendation", implements the respective guideline for business operators "covered" by the organization.

Such associations and guidelines are, despite the voluntary nature of the accreditation, relatively widespread in Japan, with many companies covered by such (sectoral) guidelines.[234]

c. Supervisory Authorities

Data protection authorities; competition authorities; economic oversight authorities.

The relevant supervisory authority for matters of personal data/information and privacy protection in Japan is the Personal Information Protection Commission (PPC),[235] under the jurisdiction of the Prime

---

[230] See Section C IV 1 c.

[231] See, for example, Art. 37 GDPR.

[232] DLA Piper Global Data Protection Laws of the World, 'Data Protection Officers in Japan' (2022) <https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=JP> accessed 11 February 2022.

[233] See Section C IV 1 c.

[234] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recitals 73-74; Personal Information Protection Commission, 'List of Authorized Personal Information Protection Organizations' (2021) <https://www.ppc.go.jp/personalinfo/nintei/list/> accessed 20 January 2022.

[235] Personal Information Protection Commission (n 68).

Minister, Art. 59 (2). It was established in 2016 as the successor of the Special Personal Information Protection Commission.[236] It is independent from the government,[237] as stated by Art. 62 APPI, and equipped with several enforcement powers.[238] Its duties are named in Art. 60 APPI as, with a list of the PPC's responsibilities contained in Art. 61 APPI. Through the possibility of formulating guidelines and rules, it also has a role as a *de facto* legislator. Notable in comparison to data protection regulators elsewhere is the collaborative and guidance-oriented approach of the PPC.[239]

The Japan Fair Trade Commission (JFTC)[240] is responsible for the enforcement of competition law, especially under the Japanese Anti-Monopoly Act, and can act in case of personal data-related competition violations.[241]

d. (Specific) Criminal Prosecution

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

Articles 82-88 APPI contain penal provisions for certain behaviors contrary to the APPI, for example Art. 83, criminalizing noncompliance with a PPC order and punishable by imprisonment of up to one year or a fine of up to 1,000,000 JPY. While the PPC has several powers of investigation,[242] it is not responsible for criminal prosecution and investigation. The PPC rather has the power to refer cases to public prosecutors or police, which will then open a criminal investigation under the Code of Criminal Procedure.[243]

e. Procedural Aspects

Investigation powers; equipment of controlling institutions.

The PPC's powers of investigation and enforcement are contained in Articles 40-46 of the APPI. While criminal investigations are not part of their responsibility,[244] Art. 40 (1) APPI gives the PPC the power to request "necessary information or material (…) or have its officials enter a business office or other necessary place (…), inquire about the handling of personal information etc., or inspect a book document and other property". Art. 40 (2) requires the official carrying out an onsite inspection to carry identification, while Art. 40 (3) clarifies that an onsite inspection is not considered a criminal investigation, which is out of the scope of the PPC's enforcement powers. Art. 43 (1) requires the PPC to properly respect "freedom of expression, freedom of academia, freedom of religion, and freedom of political activity" in the course of investigations. Articles 58-2 to 58-5 of the APPI contain more specific procedural rules, especially regarding service of documents, and with reference to the relevant rules of administrative and civil procedure.

The PPC may also appoint a "specialist commissioner" for specialized investigations as of Art. 69 APPI. Art. 78 allows the PPC to provide foreign data protection authorities with information, subject to certain

---

[236] Personal Information Protection Commission, 'Outline of the amended Personal Information Protection Act' [2016] <https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf> accessed 20 January 2022.

[237] Walters, Trakman and Zeller (n 21) 254.

[238] See *infra* Section C IV 3.

[239] Wang (n 2).

[240] Japan Fair Trade Commission, 'Home - Japan Fair Trade Commission' (17 January 2022) <https://www.jftc.go.jp/en/> accessed 26 January 2022.

[241] See *infra* Section C IV 3 b.

[242] See *infra* Section C IV 2 e.

[243] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 108.

[244] See *supra* Section C IV 2 d.

requirements and restrictions as set forth in said article.

Additionally, the accredited personal information protection organizations have the duty to "investigate circumstances surrounding the complaint" as of Art. 52 as part of the self-regulation framework concerning these accredited organizations, however, without being granted investigatory powers similar to those of public authorities, but allowed to "request the covered business operator to provide a written or oral explanation or submit a referential material" as of Art. 52 (2).[245]

3. Enforcement

a. Intervention Concerning Data Processing

Restriction and prohibition of data processing.

Articles 41 and 42 APPI contain the relevant provisions through which the PPC intervenes in cases of violations of provisions of the APPI, with the different modes of intervention listing the exact provisions for which these are applicable, respectively. Notably, provisions of the APPI which create "soft" obligations are not contained in these – however, their violation may still be considered if there is, at the same time, a violation of other provisions.[246]

Art. 41 APPI gives the PPC the right to give (non-binding) "guidance and advice". While this has no "hard" legal effect, such guidance and advice are generally followed and is very commonly used as part of the Japanese "cooperative" approach to data privacy and protection.[247] However, this "soft" approach to regulation has attracted criticism noting the "very limited evidence of use and effectiveness".[248]

Art. 42 APPI contains the mechanism for the PPC to issue recommendations and (binding) orders. To this end, there are two parallel mechanisms:[249] Under Art. 42 (1) and (2), the PPC must first issue a recommendation to allow the relevant business operator to "rectify the violation". Where the business operator does not "take action in line with the operation", the PPC may then order the taking of action.[250] In cases of more severe violations and "when recognizing there is a need to take urgent action", the PPC may issue an order under Art. 42 (3) immediately without issuing a prior recommendation and allowing the business operator to rectify the situation first. Concerning data originating from the EU, the PPC must always issue an order under Art. 42 (2) where a business operator has not complied with a recommendation.[251]

b. Intervention Concerning Business Models

Competition and economic authorities; government monopolies.

The APPI itself does not prohibit certain business models concerning data – and rules related to competition law, as common internationally, are not to be found in data

[245] See *supra* Section C IV 2 b.

[246] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 99.

[247] Wang (n 2), 674–677.

[248] Graham Greenleaf and Fumio Shimpo, 'The puzzle of Japanese data privacy enforcement' (2014) 4(2) International Data Privacy Law 139 <https://academic.oup.com/idpl/article/4/2/139/2863824?login=true> accessed 24 February 2022.

[249] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 98.

[250] Non-compliance with such an order is penalized, see *infra* Sections C IV 3 c and d.

[251] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76 (n 92), recital 101.

protection law.[252] This is exemplified by the lack of restrictions of automated processing and of data portability rights, which are commonly found in data protection laws worldwide and closely related to the regulation of business models through competition and antitrust regulation.

A rule indirectly affecting business models can, however, be found with Art. 16 (2) APPI, which requires consent of the principal in order for the continued utilization of the data in case of business successions via merger, thus limiting corporate acquisitions aimed at acquiring data held.[253]

However, the JFTC can bring action to companies under the Anti-Monopoly Act[254] on the basis that these have abused market power in relation to transactions where one side provides personal information.[255] In such cases, the JFTC may order the company to cease the violation under Art. 20 (1) of the Anti-Monopoly Act.[256]

c. Penalties for Data Processors

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

Art. 87 of the APPI concerns criminal penalties applicable as a consequence not of individual's own actions, but rather through responsibility for others, thereby allowing for fines for corporate bodies. Where a person within the scope of the corporate body's[257] responsibility, listed as "a representative (…), or an agent, employee or other worker", violates the provisions of Art. 83 to Art. 85 APPI, the corporate body may be subject to a fine alongside the individual responsible for the violation.

The 2017 version of the APPI was notable for its non-differentiation between corporate bodies and individuals regarding the amount of the fine, with the highest fines possible for companies being 500.000 JPY (currently around 3.800 EUR) under the respective articles and thus much less, if not negligible in comparison, than the towering revenue-based fines possible under the EU's GDPR.[258]

This has changed at least somewhat with the 2020 amendments to the APPI, with fines of up to 100 million JPY (currently around 775.000 EUR) possible for corporate bodies under Art. 87 (1) in cases of violations of Art. 83 or Art. 84, which concern non-compliance with an order of the PPC and illegal handling of personal information databases.[259] However, this is still much less when compared to the EU.

As the updated APPI comes has yet to come into force, it remains to be seen whether the changes in the articles will lead to significant change towards more aggressive enforcement, or whether the PPC will continue to largely rely on its "soft power".[260]

---

[252] Kentaro Hirayama and Koki Arai, 'Interaction between Information Law and Competition Law: Organizing Regulatory Perspectives on Platform Businesses' (2021) 12(2) Asian Journal of Law and Economics 171, 178.

[253] Ibid 180.

[254] Act on Prohibition of Private Monopolization and Maintenance of Fair Trade 1947, available in English at <http://www.japaneselawtranslation.go.jp/law/detail/?id=2746&vm=02&re=02&new=1> accessed 26 January 2022.

[255] See *supra* Section C III 1 c.

[256] See also Hiroshi Yamada and Masahiro Takeda, 'Report of the Study Group on data and competition policy in Japan' (2019) 9(4) International Data Privacy Law 299 <https://academic.oup.com/idpl/article/9/4/299/5599856> accessed 24 February 2022.

[257] Or an individual person's responsibility, i.e. where companies are not organized as legal entities.

[258] Niall McCarthy, 'The Biggest GDPR Fines of 2021' (5 January 2022) <https://www.eqs.com/compliance-blog/biggest-gdpr-fines-2021/#amazon> accessed 21 January 2022.

[259] See Personal Information Protection Commission, 'Comparative table of the current and amended provisions of the APPI' <https://www.ppc.go.jp/files/pdf/20200612_comparative_table_amended_APPI.pdf> accessed 21 January 2022.

[260] Wang (n 2), 678.

A more significant change, given the great importance of company reputation in the Japanese business context,[261] might be the added Art. 42 (4) APPI, whereby the PPC may publicly announce it has issued an order for noncompliance.

d. Penalties for Individual Actors

Directors' liability; individual criminal sanctions.

As follows the description above,[262] the (technical) default in the APPI is not the sanctioning of companies, but rather of individuals. These are contained in Articles 82-88 APPI, and, with the exception of the last Article, Article 88, are all criminal fines.[263] The 2020 Amendments to the APPI intensified the sanctions.[264] Article 82 allows for the most drastic of sanctions, threatening "imprisonment with work for not more than two years or a fine of not more than 1,000,000 yen" for persons who divulge or "use by stealth" secrets considered such under Art. 72, which are secrets that become known to the PPC "in the course of their duties". Thus, this provision is fairly specific and not applicable to general APPI obligations.

Art 83 APPI makes noncompliance with orders of the PPC issued under Art. 42 (2) or (3) punishable by imprisonment with labor of up to one year or a fine of 1,000,000 yen. Art. 84 APPI criminalizes "provid[ing] or us[ing] by stealth" of a personal information database etc.[265] in order to make illegal profits, which includes the "stealing" of data.[266] It was introduced as part of the 2020 amendments.[267] Art. 85 contains two items, item (i) criminalizing noncompliance with investigatory measures of the PPC under Art. 40 (1), and item (ii) the failure of accredited personal information protection organizations to report to the PPC upon request under Art. 56 APPI. Article 86 APPI clarifies that Articles 82 and 84 apply even where offenses are committed outside Japan. It should be noted that Article 87, as discussed above, applies not only for corporate bodies but also for representatives of other natural person's businesses, thus allowing for criminal sanctions even in such situations.

Finally, Article 88 of the APPI imposes a "non-criminal fine of not more than 100,000 yen" for cases of deception of a PIHBO on provision of third-party data, the use of the appellation "accredited personal information protection organization" without authorization and false submissions concerning the termination of services of such an organization.

(Indirect) individual penalties arising from violations of the APPI or data protection laws in general could also arise through the instrument of directors' liability under Japanese corporate law in case of neglecting their duties. Such liability can also extend to third parties in cases of gross negligence or knowing action.[268]

---

[261] Ibid 679.

[262] See *supra* previous section.

[263] See the wording in "Sanctions" in Hounslow and Nozaki (n 171). See also Article 88 APPI, which (contrary to the other provisions) names this a "non-criminal fine".

[264] Personal Information Protection Commission, 'Comparative table of the current and amended provisions of the APPI' (n 259).

[265] Defined in Art. 2 (4) APPI, see *supra* Section C II 1.

[266] "The amendment to the APPI (…) establishes criminal liability for providing or stealing personal information with a view to making illegal profits". (referring to Art. 84 APPI). Tomoki Ishiara, 'The Privacy, Data Protection and Cybersecurity Law Review' (5 November 2021) <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/japan#footnote-085-backlink> accessed 25 January 2022.

[267] Personal Information Protection Commission, 'Comparative table of the current and amended provisions of the APPI' (n 259).

[268] Katsuyuki Yamaguchi, Kaoro Tatsumi and Mamiko Komura, 'Corporate governance and directors' duties in Japan: overview' (1 May 2020)

e. Procedural Aspects

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

In the past,[269] and following the passing of the EU adequacy agreement, there has been criticism regarding the perceived lack of actual enforcement concerning the APPI and data privacy in Japan.[270] To this, there are two perspectives – one highlights the soft mechanisms underlying Japanese law in general[271] and the PPC in the context of the APPI,[272] stating that enforcement is simply not as necessary as elsewhere. The other perspective simply sees a lack of enforcement.[273]

However, even if one subscribes to the perspective that Japanese companies simply comply with the APPI without much "hard" enforcement, problems exist especially with foreign companies not used to the Japanese regulation by reputation/social standing approach.[274]

A trend emerges, however, by examination of the 2020 APPI amendments. These add many "hard sanctions" to the PPC's toolbox and create new responsibilities (especially breach reporting).[275] This could mean that stricter enforcement is to come. However, as the APPI amendments are yet to come into force (April 2022),[276] this remains to be seen.

<https://uk.practicallaw.thomsonreuters.com/1-502-0177> accessed 25 January 2022.

[269] Greenleaf and Shimpo (n 248).

[270] Greenleaf, 'Japan: EU Adequacy Discounted' (n 131).

[271] For a detailed examination of factors of Japanese litigiousness, see Colombo and Shimizu (n 89).

[272] Wang (n 2).

[273] Greenleaf, 'Japan: EU Adequacy Discounted' (n 131).

[274] Wang (n 2), 681.

[275] Toshiyuki Arai, 'New Amendment To Japan's Data Privacy Law (APPI)' (10 December 2020) <https://www.paulhastings.com/insights/client-alerts/new-amendment-to-japans-data-privacy-law-appi> accessed 26 January 2022; Personal Information Protection Commission, 'Comparative table of the current and amended provisions of the APPI' (n 259); Wang (n 2), 684–691.

[276] Scott W Pink, David G Litt and Yuko Zaha, 'Amended Japan Privacy Law Will Come into Effect in April 2022' (16 November 2021) <https://www.omm.com/resources/alerts-and-publications/alerts/amended-japan-privacy-law-will-come-into-effect-in-april-2022/> accessed 26 January 2022.

D. Sources and Literature

Adams AA, Murata K and Orito Y, 'The Development of Japanese Data Protection' (2010) 2(2) Policy and Internet 93.

APEC, 'Member Economies' <https://www.apec.org/about-us/about-apec/member-economies> accessed 3 February 2022.

Arai T, 'New Amendment to Japan's Data Privacy Law (APPI)' (10 December 2020) <https://www.paulhastings.com/insights/client-alerts/new-amendment-to-japans-data-privacy-law-appi> accessed 26 January 2022.

Asimov M, 'A Comparative Approach to Administrative Adjudication' in Peter Cane and others (eds), *The Oxford Handbook of Comparative Administrative Law* (Oxford University Press 2021).

Basedow J, 'AGB-Kontrolle in Japan und Deutschland' (2020) 25(49) Zeitschrift für Japanisches Recht 187–200.

Carapeto R, 'The Japanese Basic Act on Cybersecurity and the historical development of the Japanese legal framework for cybersecurity' (2021) 2(1) Int Cybersecur Law Rev 65.

Central Intelligence Agency, 'Japan - The World Factbook' (4 February 2022) <https://www.cia.gov/the-world-factbook/countries/japan/> accessed 11 February 2022.

Clermont K, 'Standards of Proof in Japan and the United States' (2004) 37(2) Cornell International Law Journal 263.

Colombo GF and Shimizu H, 'Litigation or Litigiousness? Explaining Japan's "Litigation Bubble" (2006-2010)' [2016] Oxford University Comparative Law Forum <https://ouclf.law.ox.ac.uk/litigation-or-litigiousness-explaining-japans-litigation-bubble-2006-2010/> accessed 26 January 2022.

Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L 76.

Consumer Affairs Agency, 'Outline of the Consumer Affairs Agency' <https://www.caa.go.jp/en/about_us/> accessed 3 February 2022.

Corrales M, 'Right to Know v. the Secrecy Law in Japan: Striking the Right Balance' (2014) 19(38) Zeitschrift für Japanisches Recht 189–200.

Council of Europe, 'Convention 108 in the World - Parties' (2022) <https://www.coe.int/en/web/data-protection/convention108/parties> accessed 2 February 2022.

Courts in Japan, 'Supreme Court of Japan' (28 January 2022) <https://www.courts.go.jp/english/index.html> accessed 1 February 2022.

Digital Agency, 'Outline of the Act on the Establishment of the Digital Agency' <https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_en_02.pdf> accessed 11 February 2022.

Digital Agency, 'Digital Agency' (2022) <https://www.digital.go.jp/en> accessed 3 February 2022.

DLA Piper Global Data Protection Laws of the World, 'Data Protection Officers in Japan' (2022) <https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=JP> accessed 11 February 2022.

Elbati B, 'The Supreme Court of Japan on Punitive Damages…' (2021) <https://conflictoflaws.net/2021/the-supreme-court-of-japan-on-punitive-damages/> accessed 12 January 2022.

European Commission, 'Joint statement on the first review of the EU-Japan mutual adequacy arrangement' (26 October 2021) <https://ec.europa.eu/newsroom/just/items/724795/en> accessed 11 February 2022.

Fenzel B, 'Debating the Japanese Approach to Dispute Resolution' [2011] MaxPlanckResearch Science Magazine 84 <https://www.mpg.de/4379741/W006_Culture-Society_084-091.pdf> accessed 11 February 2022.

Fujikouge T and Kosuge N, 'Amendment of Japan's Act on the Protection of Personal Information' (4 August 2020) <https://www.dlapiper.com/en/japan/insights/publications/2020/08/amendment-of-japans-act/> accessed 14 January 2022.

Fujiwara S, Geminn C and Roßnagel A, 'Angemessenes Datenschutzniveau in Japan - Der Angemessenheitsbeschluss der Kommission und seine Folgen' 2019 Zeitschrift für Datenschutz 204.

Geminn C, Laubach A and Fujiwara S, '„Schutz anonymisierter Daten im japanischen Datenschutzrecht – Kommentierung der neu eingeführten Kategorie der 'Anonymously Processed Information"" [2018] Zeitschrift für Datenschutz.

Greenleaf G, 'Japan—The Illusion of Protection' in Graham W Greenleaf (ed), *Asian data privacy laws: Trade and human rights perspectives* (1. ed. Oxford Univ. Press 2014).

Greenleaf G, 'Questioning 'Adequacy' (Pt I) – Japan' [2017] University of New South Wales Law Research Series <http://classic.austlii.edu.au/au/journals/UNSWLRS/2018/1.html>.

Greenleaf G, 'Japan: EU Adequacy Discounted' [2019] University of New South Wales Law Research Series <https://ssrn.com/abstract=3276016> accessed 13 January 2022.

Greenleaf G and Shimpo F, 'The puzzle of Japanese data privacy enforcement' (2014) 4(2) International Data Privacy Law 139.

Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc. 17 December 2019.

Hanada S, Matsuoka F and Fujiwara O, 'The top three data protection law topics in Japan: Data Protection | Spring 2020 | Legal Briefing' (2020) <https://www.inhouselawyer.co.uk/legal-briefing/the-top-three-data-protection-law-topics-in-japan/> accessed 14 January 2022.

Harald Baum, 'Rechtsdenken, Rechtssystem und Rechtswirklichkeit in Japan – Rechtsvergleichung mit Japan' (1996) 1(2) Zeitschrift für Japanisches Recht 86–109.

Higashizawa N and Aihara Y, 'Data Privacy Protection of Personal Information Versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)' (2017) 84(4) Defense Counsel Journal.

Hinz J, 'Das Recht der Mediation im japanisch-deutschen Vergleich' (2019) 24(47) Zeitschrift für Japanisches Recht 143–178.

Hirayama K and Arai K, 'Interaction between Information Law and Competition Law: Organizing Regulatory Perspectives on Platform Businesses' (2021) 12(2) Asian Journal of Law and Economics 171.

Hironaka A, 'Litigation: Japan' (20 May 2021) <https://globalarbitrationreview.com/insight/know-how/litigation/report/japan> accessed 4 February 2022.

Hounslow D and Nozaki R, 'Japan - Data Protection Overview' (2021) <https://www.dataguidance.com/notes/japan-data-protection-overview> accessed 14 January 2022.

Ishiara T, 'The Privacy, Data Protection and Cybersecurity Law Review' (5 November 2021) <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/japan#footnote-085-backlink> accessed 25 January 2022.

Iwase H, Kasai Y and Yumura S, 'Intellectual Property Rights in Japan: Overview' (1 November 2020) <https://uk.practicallaw.thomsonreuters.com/5-501-5659> accessed 4 February 2022.

Japan Broadcasting Corporation (NHK), 'NHK Corporate Information' (18 June 2021) <https://www.nhk.or.jp/corporateinfo/> accessed 3 February 2022.

Japan Fair Trade Commission, 'Home - Japan Fair Trade Commission' (17 January 2022) <https://www.jftc.go.jp/en/> accessed 26 January 2022.

Japan Patent Office, 'The Role of the Japan Patent Office' (13 August 2021) <https://www.jpo.go.jp/e/introduction/soshiki/yakuwari.html> accessed 3 February 2022.

Kellner M, 'Legal Education in Japan, Germany and the United States: Recent Developments and Future Perspectives' (2007) 12(23) Zeitschrift für Japanisches Recht 195–205.

Kinoshita T, 'Legal System and Legal Culture in Japan' (2001) 6(11) Zeitschrift für Japanisches Recht 7–36.

Kirchhoff U and Schiebe T, 'The Reform of the Japanese Act on Protection of Personal Information. From the Practitioner's Perspective' (2017) 22(44) 1 199–212.

Kitagawa Z, 'Introduction: The Identity of Japanese and German Civil Law' in Zentaro Kitagawa and Karl Riesenhuber (eds), *The Identity of German and Japanese Civil Law in Comparative Perspectives/ Die Identität des deutschen und des japanischen Zivilrechts in vergleichender Betrachtung* (de Gruyter Recht 2007).

Komukai T, 'Data Protection in the Internet: Japanese National Report' in Dário Moura Vicente and Sofia de Vasconcelos Casimiro (eds), *Data Protection in the Internet* (vol 38. Springer International Publishing 2020).

Kudo T, 'Group Litigation (Class Action) in Japan' in Keio Insitute for Global Law and Development (ed), *How Civil Law Is Taught in Asian Universities* (Programs for Asian Global Legal Professions Series. Keio University Press 2019).

Kuner C, 'Article 45' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *Commentary on the EU General Data Protection Regulation* (Oxford University Press 2020).

Matsui S, 'Fundamental Human Rights and 'Traditional Japanese Values': Constitutional Amendment and Vision of the Japanese Society' (2018) 13(1) Asian J Comp Law 59.

Matsuoka F and others, 'Atsumi & Sakai Newsletter | Amendments to the Act on the Protection of Personal Information' (2021) <https://www.aplawjapan.com/application/files/5816/3339/3524/Newsletter_AS_016.pdf> accessed 14 January 2022.

McCarthy N, 'The Biggest GDPR Fines of 2021' (5 January 2022) <https://www.eqs.com/compliance-blog/biggest-gdpr-fines-2021/#amazon> accessed 21 January 2022.

McCurry J, 'Abe defends Japan's secrets law that could jail whistleblowers for 10 years' *The Guardian* (10 December 2014) <https://www.theguardian.com/world/2014/dec/10/japan-state-secrets-law-security-dissent> accessed 13 January 2022.

Ministry of Internal Affairs and Communications, 'Guidance on the Ministry of Internal Affairs and Communications' (21 February 2020) <https://www.soumu.go.jp/english/soumu/index.html> accessed 3 February 2022.

Ministry of Justice J, 'Japanese Law Translation - [Law text] - Civil Code' (2009) <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2057&re=02&vm=02> accessed 12 January 2022.

Ministry of Justice of Japan, 'PSIA' (15 September 2021) <https://www.moj.go.jp/psia/English.html> accessed 3 February 2022.

Miyashita H, 'EU-Japan Mutual Adequacy Decision' Blog Droit Européen <https://blogdroiteuropeen.files.wordpress.com/2020/06/miyashita-redo.pdf> accessed 11 February 2022.

Miyashita H, 'The evolving concept of data privacy in Japanese law' (2011) 1(4) International Data Privacy Law 229.

Morimoto D and Hamano T, 'Confidentiality Q&A: Japan' (2020) <https://uk.practicallaw.thomsonreuters.com/w-027-0037> accessed 13 January 2022.

Nakada M and Tamura T, 'Japanese Conceptions of Privacy: An Intercultural Perspective' (2005) 7(1) Ethics Inf Technol 27.

NICT - National Institute of Information and Communications Technology, 'NICT - Home' (7 February 2022) <https://www.nict.go.jp/en/> accessed 7 February 2022.

NISC, 'National center of Incident readiness and Strategy for Cybersecurity | About NISC' (1 February 2022) <https://www.nisc.go.jp/eng/index.html#sec1> accessed 3 February 2022.

Oda H, *Japanese Law* (4th edn, Oxford University Press 2021).

OECD, 'About the OECD' (5 January 2022) <https://www.oecd.org/about/> accessed 3 February 2022.

Okada A, 'Japan's legal approach to data transactions - SOLAIR Conference 2020' (10 September 2020) <https://solairconference.com/data/files/Japan-legal-approach-to-data-transactions.pptx>.

Okuhara K, 'Researching Japanese Law - GlobaLex' (12.2020) <https://www.nyulawglobal.org/globalex/Japan1.html> accessed 4 February 2022.

Orito Y and Murata K, 'Privacy Protection in Japan: Cultural Influence on the Universal Value' [2005] *Proceedings of ETHICOMP* <http://www.isc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf>.

Orito Y, Murata K and Young CA, 'E-Governance Risk in Japan: Exacerbation of Disciriminative Structure Built in the Family Registration System' in Terrell Ward Bynum and others (eds), *ETHICOMP 2013 Conference Proceedings: The possibilities of ethical ICT* (2013).

Parashar C, 'Japan's Digital Agency: Another shot in the dark or an emblem of change' *Observational Research Foundation* (11 November 2021) <https://www.orfonline.org/expert-speak/japans-digital-agency/> accessed 3 February 2022.

Personal Information Protection Commission, 'Comparative table of the current and amended provisions of the APPI' <https://www.ppc.go.jp/files/pdf/20200612_comparative_table_amended_APPI.pdf> accessed 21 January 2022.

Personal Information Protection Commission, 'Current Legal Framework of the Protection of Personal Information' <https://www.ppc.go.jp/files/pdf/280222_Current_Legal_Framework_v2.pdf> accessed 2 February 2022.

Personal Information Protection Commission, 'Laws and Policies' <https://www.ppc.go.jp/en/legal/> accessed 11 February 2022.

Personal Information Protection Commission, 'Roles and Responsibilities' <https://www.ppc.go.jp/en/aboutus/roles/> accessed 20 January 2022.

Personal Information Protection Commission, 'Outline of the amended Personal Information Protection Act' [2016] <https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf> accessed 20 January 2022.

Personal Information Protection Commission, 'List of Authorized Personal Information Protection Organizations' (2021) <https://www.ppc.go.jp/personalinfo/nintei/list/> accessed 20 January 2022.

Pink SW, Litt DG and Zaha Y, 'Amended Japan Privacy Law Will Come into Effect in April 2022' (16 November 2021) <https://www.omm.com/resources/alerts-and-publications/alerts/amended-japan-privacy-law-will-come-into-effect-in-april-2022/> accessed 26 January 2022.

Prime Minister of Japan, 'Toward a New Era of "Hope-Driven Economy": The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting' (23 January 2019) <https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html> accessed 11 February 2022.

Sagara Y, 'Big Data Protection under Unfair Competition Prevention Act has just started in Japan' (2019) <https://www.nakapat.gr.jp/ja/legal_updates_eng/big-data-protection-under-unfair-competition-prevention-act-has-just-started-in-japan/> accessed 11 February 2022.

Schwartz PM, 'Global Data Privacy: The EU Way' [2019] NYU Law Review 772 <https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf> accessed 10 January 2022.

Sorte WF, 'Does the Japanese inclination towards non-litigation hinder access to justice for minority groups?' (2014) 4(3) IJPLAP 221.

Suzuki A, 'Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Japan' (27 October 2021) <https://uk.practicallaw.thomsonreuters.com/w-026-4239> accessed 3 February 2022.

Tanaka H and Kitayama N, 'Japan enacts Amendments to the Act on the Protection of Personal Information' (2020) <https://iapp.org/news/a/japan-enacts-the-act-on-the-protection-of-personal-information/> accessed 20 January 2022.

Tanaka H, Tsuta D and Shimamura N, 'Cybersecurity Comparative Guide' (13 August 2020) <https://www.mondaq.com/technology/976226/cybersecurity-comparative-guide> accessed 11 February 2022.

United Nations, 'Member States' <https://www.un.org/en/about-us/member-states> accessed 3 February 2022.

Wada T, 'Data Protection in Japan' (Turning Point in Data Protection Law).

Walters R, Trakman L and Zeller B, 'Japan' in Robert J Walters, Leon E Trakman and Bruno Zeller (eds), *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches: European Union, Singapore, Australia, India, Indonesia, Malaysia, Thailand, Japan* (Springer 2019).

Wang FY, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' [2020] Harvard Journal of Law & Technology 661 <https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf> accessed 10 January 2022.

Watson ARJ, 'Changes in Japanese Legal Education' (2016) 21(41) Zeitschrift für Japanisches Recht 1–54.

Wong M and Kawakami I, 'Japan - Individual - Tax administration' (16 August 2021) <https://taxsummaries.pwc.com/japan/individual/tax-administration> accessed 27 January 2022.

World Intellectual Property Organization, 'WIPO-Administered Treaties - Contracting Parties < Japan' <https://wipolex.wipo.int/en/treaties/ShowResults?country_id=87C> accessed 11 February 2022.

World Intellectual Property Organization, 'Information by Country: Japan' (8 December 2021) <https://www.wipo.int/members/en/details.jsp?country_id=87> accessed 3 February 2022.

World Trade Organization, 'WTO Members and Observers' (13 August 2018) <https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm> accessed 3 February 2022.

Yakura C and Teraguchi Y, 'Litigation and Enforcement in Japan: Overview' (2021) <https://uk.practicallaw.thomsonreuters.com/9-502-0319>.

Yamada H and Takeda M, 'Report of the Study Group on data and competition policy in Japan' (2019) 9(4) International Data Privacy Law 299.

Yamaguchi K, Tatsumi K and Komura M, 'Corporate governance and directors' duties in Japan: overview' (1 May 2020) <https://uk.practicallaw.thomsonreuters.com/1-502-0177> accessed 25 January 2022.

Zufall F, *Planungsrecht im Vergleich* (Beiträge zum ausländischen und vergleichenden öffentlichen Recht Band 37, 1. Auflage, Nomos Verlagsgesellschaft 2015).

Zufall F, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (2019) 5(1) European Data Protection Law Review 17.