The Japanese Regulations on Data Transfer toward Data Free Flow with Trust

Hiroshi Miyashita
Professor of Law, Faculty of Policy Studies, Chuo University
Email: hmiya.64r@g.chuo-u.ac.jp

This paper was prepared with support from the Digital Freedom Fund for the Digital Trade Alliance workshop 'Europe Asia-Pacific Data Privacy and Trade: focus on Japan' on 21 June 2022. The author would like to express gratitude to Mr. Javier Ruiz for his insightful suggestions on draft paper and to the participants for their valuable comments at the workshop. The views and conclusions are those of the author.

Executive Summary

This paper explains the Japanese regulations on data transfer and examines the potential impact to data protection and transfer from trade agreements. It also considers the meaning of the Data Free Flow with Trust (DFFT) initiative and its impact on the existing data transfer tools.

In chapter I, this paper clarifies the complex regulations regarding data transfer from Japan to a third country under the Act on the Protection of Personal Information (APPI) and the Personal Information Protection Commission (PPC)'s rules. In sum, the recipient party in a foreign country ensures the level of protection according to the eight principles of the OECD Privacy Guidelines; whether the third country benefits from the adequacy decision or the APEC CBPR system, this becomes proof of secure data transfer under the APPI.

Chapter II deals with the issues relating to the crossroads of trade agreements and data protection law. For instance, data localization is prohibited in some agreements while others allow it. Some new agreements contain controversial clauses from a data protection perspective, such as a prohibition against accessing the source code or algorithm since data protection law provides access rights including meaningful information of the logic involved in the automated decision making. With regards to the solutions of cross-border data flow in the WTO, the existing data transfer regulatory frameworks will meet this general exception clause without constituting 'a means of arbitrary or unjustifiable discrimination'. First, personal data has been protected as a fundamental right as a necessary measure, second, cross-border data flow regulation is permissible and authorised by a wide-range of international instruments, and third the regulatory frameworks including the GDPR prepare for several alternative options for transferring personal data other than the adequacy decision.

Chapter III examines the DFFT initiative and the PPC's global strategy on global certification for corporations. The PPC aims to establish'the global certification system' as 'a core of PPC's global strategy' with an aim of allowing 'different frameworks such as GDPR or APEC CBPR to coexist, and be inclusive, not exclusive' However, a question may arise if the DFFT calls for WTO intervention as a dispute resolution agency in the context of cross-border data flow. DFFT may be successful in the future if it is debated solely at the WTO but an international fora for realising human-centric data protection law.

The Japanese data transfer regulations may set a mild standard compared with the EU GDPR, which may become a reason why the flexibility of the Japanese approach is tolerant about, seemingly incompatible, diverse trade agreements.

1. Data Transfer Regulation under the APPI

1. Overview of the APPI's developments and the amendments in 2020

The hierarchy of the Japanese personal information protection system was supported by the Constitution of Japan at its highest level. While the Constitution does not explicitly mention the right to privacy nor the right to data protection, a series of the Supreme Court judgements affirmed that the privacy interest is protected under the personality right of the Article 13 of the Constitution as well as the search and seizer clauses of Article 35 in the criminal investigation cases. The legislations regarding the personal information protection must comply with constitutional principles. Any guidelines and administrative rules can be provided within the scope and legal grounds of the Acts but are understood as not legally binding instruments, including the Supplementary Rules for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision[1]. The relationship between the domestic law and international law or international trade agreements are complex, however, it is generally understood that international agreements should be authorized, before its entry into force, by the Diet, the Japanese Parliament, to be incorporated into the national law as was the case in the Council of Europe's Cyber Crime Convention. Non-binding international instruments such as the OECD Privacy Guidelines and the APEC Privacy Frameworks are valuable reference for the Japanese personal information protection laws, which have no direct effect as domestic laws. The EU adequacy decision may also be regarded as an international soft-law for a third country like Japan, however, since the potential extraterritorial effect to the Japanese controllers under the GDPR and the Japanese government also provided assurance documents, it has been regarded as having a quasi-binding international effect for Japanese stakeholders.

The personal information protection system was initially seen in local ordinances in the 1970s followed by, at the national level, the Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs of 1988, which was later replaced by the Act on the Protection of Personal Information Held by Administrative Organs of 2003. In 2003, the comprehensive personal information protection system was realised with both private sector (The Act on the Protection of Personal Information) and public sector (The Act on the Protection of Personal Information Held by Administrative Organs/ The Act on the Protection of Personal

[1] PPC, 'Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision' <https://www.ppc.go.jp/files/pdf/supplementary_rules.pdf>.

Information Held by Incorporated Administrative Agencies) legislation.

The Act on the Protection of Personal Information (APPI) of Japan of 2003 was amended in 2015, 2020 and 2021. The 2015 amendments to the APPI had the clear aim of obtaining an adequacy decision from the European Commission. The 2020 amendments to the APPI were mandated by the every-three-year review of the APPI's Supplementary Provision[2], while the 2021 amendments occurred because of establishing the new Digital Agency in September 2021. These amendments were obviously motivated by harmonisation with the international developments in data protection, in particular the EU's General Data Protection Regulation (GDPR).

In the international data transfer context, the Japanese government proposed pursuing the adequacy decision under the EU GDPR (then Data Protection Directive) in April 2015[3]. On 23 January 2019, the European Commission issued an adequacy decision to the APPI together with the Supplementary Rules and written commitments by Japanese high officials. The PPC published a list of 30 EEA countries and the UK as ensuring the equivalent level of protection of personal information in third countries under the APPI[4]. On the very same day, the Japanese data strategy of 'Data Free Flow with Trust' was proposed by then-Prime Minister Abe at the World Economic Forum, later endorsed by the G20, which aims to promote free flow of data across borders by ensuring the protection of privacy, security and intellectual property[5].

The APPI amendments and the Personal Information Protection Commission (PPC)'s agenda are consistent with the international harmonization. These amendments are, among others, (i) strengthening data subjects' rights such as cessation of utilisation or deletion, (ii) abolishing the short-term data within six months exemption, (iii)

---

[2] APPI Supplementary Provisions on Art. 12 (3) (9 September 2015). 'The government shall take necessary measures every three years after entry of this Act, if necessary, based on the result of the examinations regarding the implementation status of the new Act on the Protection of Personal Information by considering the international developments on the protection of personal information, ICT developments, and the following circumstances of creating and developing the new industry by utilising personal information'

[3] Then-Minister Shunichi Yamaguchi expressed in the House of Representatives that 'the government will proceed to obtain the adequacy finding from EU in order to improve the Japanese business environment in EU after the bill passes through'. Plenary Session, House of Representatives, Diet 189, 23 April 2015, Minister Shunichi Yamaguchi.

[4] PPC, 'Foreign Countries of the system of the protection of personal information which are recognised as ensuring the equivalent to Japan in protecting rights and interests of an individual (Notice No.1, 2019) (「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国等」)'. <https://www.ppc.go.jp/files/pdf/200201_h31iinkaikokuji01.pdf> (in Japanese).

[5] MOFA, 'Speech by Prime Minister Abe at the World Economic Forum Annual Meeting' 23 January 2019. <https://www.mofa.go.jp/ecm/ec/page4e_000973.html>

introducing pseudonymous processing information for data utilisation, (iv) clarifying data subjects' consent for utilization of personal data in the case of a Data Management Platform (DMP), (v) introducing mandatory data breach notification, (vi) prohibiting inappropriate utilisation of personal data, (vii) extending the information to be provided in the case of transferring personal data to the third countries, and (viii) lifting the amount of fines up to 100 million yen (approximately 770,000 euro).

2. Legislative framework of data transfer under the APPI

2-1. Legal grounds for transferring personal data under the APPI

Data transfer restrictions were introduced in the 2015 APPI amendments. Before these amendments, there were several incidents and concerns regarding data transfer. For instance, in 2009, more than 32 thousand pieces of customer data were leaked from a Chinese company trusted by the Alico Japan insurance company. Concern was also raised in establishing a joint holding company in 2014 between Japanese Panasonic Health Care and the US Kohlberg Kravis Roberts & Co for transferring medical data of Japanese patients to the US.

By the 2015 amendments, personal data can be exported to a third party in a foreign country if one of the following items is met: namely,

1) where the data subjects consent,

2) where business operator establishes a system conforming to the standards prescribed by the PPC's rules, or

3) where the third country ensures the equivalent standards to the Japanese personal information protection system (Art. 28 (1))[6]. The EEA's 30 countries and the UK met this third requirement based on the mutual adequacy decision.

2-2. Consent of data subjects

[6] 'A personal information handling business operator, except in those cases set forth in each item of the preceding Article, paragraph (1), shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section (referred to as "equivalent action" in paragraph (3)) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests; hereinafter the same in this Article and the succeeding paragraph), in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.' (Art. 28(1)).

In the following 2020 amendments, additional requirements were incorporated for the business operators in exporting personal data to a third country. Regarding the data subjects' consent, business operators must provide information on the personal information protection system of the foreign country in advance (Art.28(2))[7]. This information should be provided by electromagnetic record, document or in other proper ways (PPC Rules Art.17(1)). This information should contain the name of the third country, its personal information protection system of the third country, and the measures taken by the third party in a foreign country (PPC Rules Art. 17 (2)). In a case where the country at the time of obtaining consent is not identified, the business operator must provide its reason and any reference information, if any (PPC Rules Art.17(3)).

2-3. Standard under the PPC's Rules: compliance to the APPI obligations or certification

With regards to a system established by a business operator, the PPC's Rule clarifies relevant standards: either the importer ensures the obligations prescribed by the APPI chapter 4 section 2 in a proper and reasonable way or the importer receives a certification under an international framework (PPC Rules Art. 16). Thus, the PPC Rules' standards provide two options for the business operators to transfer personal data.

Regarding the standards for an importer to properly and reasonably ensure adherence to APPI obligations, the PPC's Guidelines exemplify the contract or MoU between the exporter and the importer in a foreign country, or the common privacy policy within the same corporate group. The Guidelines also note that the OECD Privacy Guidelines as well as the APEC Privacy Framework must be considered in assessing fulfilment of the obligations in a proper and reasonable way under the APPI. The PPC Guidelines further explain that the exporter's APEC CBPR's certification can fufil the requirements of implementing the APPI's obligations in a proper and reasonable way[8].

The other option for certification under the international framework is based on the PPC's Rules; the PPC only names certification by the APEC CBPR system, if the importer

---

[7] 'A personal information handling business operator shall, in case of intending to obtain a principal's consent pursuant to the provisions of the preceding paragraph, in advance provide the principal with 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 a reference to the principal, pursuant to rules of the Personal Information Protection Commission'. (Art. 28(2)).

[8] PPC, 'Guidelines on the Act on the Protection of Personal Information (Transfer to the third party in a foreign country edition) (「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」)' (November 2016, last revised October 2021) 9. <https://www.ppc.go.jp/files/pdf/211029_guidelines02.pdf> (in Japanese).

in a foreign country obtains this, as a valid transfer[9].

2-4. PPC's decision regarding equivalent level of protection in the third country

Regarding data transfer based on equivalent standards, which were clarified before the 2020 amendments, the PPC Rules provide five necessary criteria (PPC Rules Art. 15). The third country must: 1) have laws regulating the business operator's handling of personal information and its implementation; 2) ensure the existence of an independent authority equivalent to the PPC and its necessary and proper supervision; 3) cooperate with Japan based on a mutual understanding on the utilisation of personal information and protection of individual rights and interests; 4) ensure mutual data flow with protection of personal information without restricting international data transfer beyond the scope necessary to protect personal information; and 5) contribute to the new innovation and economic society as well as the realisation of life for the Japanese citizen. The PPC prepared an assessment report on the EU member states before the mutual adequacy decision, though this was not published[10]. As mentioned earlier, the EEA 30 countries plus the UK were recognised as ensuring these criteria by the PPC's decision. It has not reviewed the additional trading partners for an equivalency decision.

2-5. PPC's preparation for the amended APPI

PPC prepared for the implementation of these 2020 amendments for an entry into force on 1 April 2022. For instance, the PPC revised the Guidelines for transfers to a third party in a foreign country edition on 29 October 2021 in accordance with the 2020 amendments[11]. There has been no change in the referred international frameworks such as the OECD Privacy Guidelines, the APEC Privacy Framework, and the international certification of the APEC CBPR system after the mutual adequacy decision in 2019.

In March 2021, the major social media corporation, LINE, with 86 million users in Japan allowed the Chinese contracting company to access personal data with a possibility of surveillance by a Chinese government; they also transferred personal data to South Korea without mentioning it in their privacy policies. The PPC issued an administrative instruction against LINE, pointing out that it failed to provide sufficient security measures

---

[9] Ibid 39.
[10] PPC, Report on Assigning the EU based on Article 24 of the Act on the Protection of Personal Information, 18 January 2019 (「個人情報の保護に関する法律第 24 条に基づくＥＵの指定に関する報告書」) <https://www.ppc.go.jp/files/pdf/310118_siryou1-1.pdf> (in Japanese).
[11] Ibid.

and supervision over the foreign trustee[12]. Although the main issue in the LINE case was data transfer, the PPC could not mention it because of the 2020 amendments awaited entry into force at that time. In any event, the LINE data scandal caused a restructuring of the data governance system[13] and envisages risks in data transfer for other Japanese global companies.

2-6. PPC's Survey on data transfer

The PPC has previously conducted several study of the legislative developments in the foreign countries. For instance, before the PPC recognised the EEA's adequacy, the PPC prepared a report on the legal regime and its implementations in the 31 EEA countries[14]. Later, the PPC provided several research reports in the foreign countries such as 'Report on the developments regarding the GDPR implementation and its measures in the EU'[15] in 2019 and 'Report on the implementation regarding transfer of personal data among Japan, the U.S. and the EU'[16] in 2022. The 2022 survey for the 113 Japanese corporations belonging to the Japan Business Federation shows that 66.4 percent of them have received personal data from the EU[17]. Among these, 39.7 percent (in total 26.5 percent of all the companies) circulate personal data from the EU to the U.S. via Japan[18]. This report contains several interviews with the corporations, none of which relied on the APEC CBPR system for transfer to the US. These research studies also include EU and US legislative developments with a full translation of the GDPR and California Consumer

---

[12] PPC, 'Regarding administrative response under the Act on the Protection of Personal Information 「個人情報の保護に関する法律に基づく行政上の対応について」' 23 April 2021 <https://www.ppc.go.jp/files/pdf/210423_houdou.pdf> (in Japanese).

[13] Z Holdings, 'Final Report by the Special Advisory Committee on Global Data Governance' 18 October 2021. https://www.z-holdings.co.jp/notice/20211018 (in Japanese).

[14] PPC, 'Report on Designating the EU under Article 24 of the Act on the Protection of Personal Information (「個人情報の保護に関する法律第 24 条に基づく ＥＵの指定に関する報告書」)' https://www.ppc.go.jp/files/pdf/310118_siryou1-1.pdf (in Japanese).

[15] PPC, 'Report on the developments regarding the GDPR implementation and its measures in the EU (「EU における GDPR（一般データ保護規則）の運用及び対応に関する動向調査調査報告書」)' 29 March 2019. <https://www.ppc.go.jp/files/pdf/gdpr-doukou-report.pdf> (in Japanese) (conducted by Nomura Research Institute).

[16] PPC, 'Report on the implementation regarding transfer of personal data among Japan, the U.S. and the EU (「日米欧における個人データの越境移転に関する実態調査調査結果報告書」)' 27 January 2022 <https://www.ppc.go.jp/files/pdf/nichibeiou_ekkyouiten_report.pdf> (in Japanese) (conducted by Nomura Research Institute).

[17] Ibid 12. (93.3 percent of them are group corporations and 37.3 percent of them are outside their own corporations (multiple answers)).

[18] Ibid 1 & 16 (30 companies out of 113 answered that they made onward transfer from the EU to the US).

Privacy Act[19]. Alongside with these research reports, in 2022, the PPC published a study report of 34 jurisdictions of the personal information protection systems and the regulation of government access to private date[20].

The PPC's Guidelines state that 'in transferring personal data across borders, it is important for the business operator as a data exporter to provide intelligible information to the principal [data subject] by assessing the risks entailed in transferring personal data to a third party as an importer within a foreign country and considering the necessity of such transfer' under the PPC Rules (Art. 17(2))[21].

Three items must be provided to data subjects according to the PPC's Rules (Art. 17(2)). First, the name of the transferred country. If the business operator cannot identify the foreign country in time to obtain consent from data subjects (e.g. a Japanese pharmacy company cannot identify the final approval country for medical research when a doctor attempts to obtain consent from a data subject), they must attest to its impossibility and the reason to the data subjects (PPC Rules Art.17(3)).

Secondly, as an exporter, the business operator must provide information regarding the protection of personal information in the foreign country, obtained in a proper and reasonable way. Information on the foreign system to data subjects must be obtained in a proper and reasonable way in order to give predictability for the data subjects such as referring to the third party in the foreign country or confirming the published information by the Japanese or foreign administrative institutions[22]. The PPC Guidelines recognise sufficient information to data subjects as the adequacy countries decided by the European Commission or the member economies of the APEC CBPR system[23]. In case where this objective information is lacking, the business operator as an exporter must provide information to data subjects if the foreign system lacks the obligations or rights corresponding to the eight principles of the OECD Privacy Guidelines[24], which proves

---

[19] Translations are available at https://www.ppc.go.jp/enforcement/infoprovision/laws/

[20] PPC, Study on the Systems on the Protection of Personal Information in the Foreign Countries (「外国における個人情報の保護に関する制度等の調査について」), 17 September 2021 and 10 February 2022.
https://www.ppc.go.jp/files/pdf/210917_pp_offshore_kouhyou_sywkqc.pdf
https://www.ppc.go.jp/files/pdf/220210_pp_offshore_kouhyou_sywkqc.pdf

[21] PPC, 'Guidelines on the Act on the Protection of Personal Information (Transfer to the third party in a foreign country edition)' (November 2016, last revised October 2021) 40. <https://www.ppc.go.jp/files/pdf/211116_guidelines01.pdf> (in Japanese).

[22] Ibid 42.

[23] Ibid 43.

[24] The eight OECD privacy principles are collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle and accountability principle. OECD, 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of

the essential difference from the Japanese APPI[25]. Any additional information which may affect data subjects, including the obligation to cooperate with the government surveillance or data localisation to prohibit erasure of transferred data, must also to be provided.

Third, the business operator must provide information regarding the measures taken by the third party in a foreign country to protect personal information. It is sufficient to provide the factual information if the third party takes measures according to the eight principles of the OECD Privacy Guidelines. However, if the third party in a foreign country cannot ensure the measures corresponding to the OECD's eight privacy principles, such failure information must be provided to data subjects[26].

The business operator as an exporter must continue to monitor and periodically check the measures taken by a third party in a foreign country (Art. 28(3), PPC Rules 18).

With these new data transfer regulations, on 17 September 2021, the PPC noted that a report would be prepared by the end of 2021 in order to provide the Japanese companies which should give information to data subjects regarding the legal regime of an intended data export country in accordance with the 2020 amendments[27]. The PPC explains that they chose 31 countries/regions based on the result of survey regarding transfer of personal data among the Japanese corporations.

3. Summary

From the PPC's documents and guidelines, the common criteria of transfer assessment can be found at geographical and organizational levels. From a geographical perspective, the PPC sets the criteria for EU adequacy countries and the countries of participating in the APEC CBPR system. Regarding the organisational criteria for transferring personal data, the PPC clearly relies on the eight principles in the OECD Privacy Guidelines as the main criteria for assessing data transfer risks unless the third country obtains an EU adequacy decision or participates in the APEC CBPR system. Therefore, if the country transferring personal data from Japan either obtains an adequacy decision by the EU or participates the APEC CBPR system, this is sufficient to obtain consent from data subjects. If the third country does not meet this standard, the business

---

Personal Data' (1980 revised in 2013). <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

[25] PPC, 'Guidelines on the Act on the Protection of Personal Information (Transfer to the third party in a foreign country edition)' (November 2016, last revised October 2021) 43.

[26] Ibid 45.

[27] PPC, Regarding the research on the system of the protection of personal information in foreign counties（「外国における個人情報の保護に関する制度等の調査について」）17 September 2021. https://www.ppc.go.jp/files/pdf/210917_pp_offshore_kouhyou_sywkqc.pdf (in Japanese).

operator must demonstrate the importer's compliance level based on the eight principles of the OECD Privacy Guidelines.

In practice, it is important to scrutinise the data strategy of Japanese corporations. As of 1 April 2022, only three Japanese companies (Intasect, Paidy and Yahoo Japan)[28] so far received certifications from JIPDEC as an Accountability Agent under the APEC CBPR system. While the EU's GDPR has been the most influential international instrument among Japanese global companies, some of them may choose the other paths from the corporate strategy. Yahoo Japan, one of the leading internet companies in Japan, recently clarified its data strategy by quitting the services in the EU and instead obtained the APEC CBPR certification in January 2022. Yahoo Japan did not explain its reasoning, however, it is obvious that they may not be able to comply with the GDPR in the future.

A crucial question may arise as to the PPC's position on the compatibility between the EU adequacy decision and the APEC CBPR system. Thus far, the PPC seems to allow both options of the EU adequacy decision and the APEC CBPR on the same page as effective tools of transferring personal data from Japan to a third county. The PPC does not explain its compatibility. Optimistically, the PPC will accept all the relevant international frameworks together and may raise all these standards to the level of APPI's compliance as a high standard, if it believes the APPI sets one of the highest standards for protecting personal data. From a pessimistic view, the PPC's will not consider the incompatibility of the elements between the EU adequacy decision and the APEC CBPR such as their binding/non-binding nature and enforcement actions against noncompliance. Under a pragmatic approach, the PPC has been referring to the available international frameworks for global Japanese companies, depending on the directions of data transfers, the volume and sensitivity of personal data transferred to a third country, and the risks of abusing or leaking personal data after exporting from Japan to a third country.

To put it simply, the recipient party in a foreign country ensures the level of protection according to the eight principles of the OECD Privacy Guidelines. Whether it benefits from the adequacy decision or the APEC CBPR system or not, this becomes proof of secure data transfer under the APPI. If so, it is reasonable to conclude that the PPC's regulatory framework of transferring personal data leaves a huge flexibility for the business operators since the OECD privacy principles are universal but adaptable and versatile for the different legal regimes.

---

[28] The list of the APEC CBPR certifications by the JIPDEC (Japan Information Processing and Development Center) is available at https://english.jipdec.or.jp/protection_org/cbpr/list.html

2. Cross-Border Data Flow in the Context of Japan-EU Relations

2-1. An Overview of the Japanese Economic Diplomacy

Japan has been engaging with several international fora to promote economic diplomacy. As a member of G7, G20, the Organisation for Economic Co-operation and Development (OECD), and World Trade Organisation (WTO), Japan participates international frameworks of free trade and investment. Japan also promotes the Economic Partnership Agreement (EPA)/ Free Trade Agreement (FTA) via 21 existing EPAs/FTAs and related initiatives (Singapore, Mexico, Malaysia, Chile, Thailand, Indonesia, Brunei, ASEAN, the Philippines, Switzerland, Viet Nam, India, Peru, Australia, Mongolia, the Trans-Pacific Partnership (TPP)12 (signed), the TPP11, the EU, the US, the UK (signed), the Regional Comprehensive Economic Partnership Agreement (RCEP) (signed)) [29]. Statistics show China, the US and the EU are Japan's main trade partners[30].

Top Trade Counterparts Countries in 2020

	Export	Import
1	China 3,258 (23.9)	China 1,750 (25.7)
2	U.S.A. 2,006 (14.7)	U.S.A. 745 (11.0)
3	South Korea 760 (5.6)	Australia 383 (5.6)
4	Taiwan 760 (5.6)	Taiwan 286 (4.2)
5	Thailand 526 (3.9)	South Korea 284 (4.2)
- (region)	EU 1,429 (10.5)	EU 783 (11.5)

million JPY (percentage of the total sum)

Each international for a exerts a potential impact on data privacy. For instance, most recently, a meeting of the G7 data protection and privacy authorities was held in September 2021, resulting in the publication of agreed outcomes related to privacy and competition, shaping the future of online tracking and designing artificial intelligence in line with data protection[31]. Japan also led the G20 meeting in 2019 where the Osaka Declaration was adopted under an initiative of 'Data Free Flow with Trust'[32].

---

[29] Ministry of Foreign Affairs of Japan, Free Trade Agreement (FTA) / Economic Partnership Agreement (EPA) and Related Initiatives https://www.mofa.go.jp/policy/economy/fta/index.html.
[30] Trade statistics are available at Customs and Tariff Bureau homepage < https://www.customs.go.jp/toukei/info/index_e.htm>.
[31] G7 data protection and privacy authorities' meeting: communiqué https://ico.org.uk/media/about-the-ico/documents/4018242/g7-attachment-202109.pdf
[32] G20's Osaka Leaders' Declaration

Japan has also been actively participated in OECD frameworks. The original 1980 OECD Privacy Guidelines (amended in 2013) are the most credible international reference for drafting the Japanese APPI. With regard to cross-border cooperation, Japan supported the 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' in 2007 and joined the Global Privacy Enforcement Network (GPEN) to share best practices for addressing cross-border challenges. The Japanese PPC also hosted an OECD event, which recently produced a statement on government access to personal data held by the private sector[33].

With regard to the Asia-Pacific, the Asia Pacific Economic Cooperation (APEC) established the privacy rules pertaining to e-commerce in 2005 known as the 'APEC Privacy Framework' which was amended in 2015[34]. The APEC Cross-Border Privacy Rules (CBPR) system was created in 2011 at the APEC Leaders Meeting. It includes a certification mechanism for cross-border data transfers for trade benefits. Japan joined the APEC CBPR in 2014 with other seven economies (Australia, Chinese Taipei, Canada, the Republic of Korea, Mexico, Singapore and the United States). In the CBPR system, certification was given by the Accountability Agent. The Japan Information Processing Development Center (JIPDEC) has issued over 16,000 domestic Japanese companies 'PrivacyMark' certifications since 1998[35]. JIPDEC also published a certification standard for the APEC CBPR in December 2016[36] based on the APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines. In the CBPR system, only three Japanese companies have been accredited so far.

While the WTO is not primarily a forum for resolving human rights issues including the right to privacy and personal data protection, the Japanese government has insisted that the WTO may play a role in promoting the free flow of data without non-tariff barriers. In 2019, then Prime Minister Shinzo Abe stated that digital governance challenges related to privacy, data protection, intellectual property rights, and security should be addressed 'under the roof of the WTO'[37].

Application of the Japanese regional economic cooperation strategy is observable

---

<https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html>.

[33] OECD, Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy, December 2020. https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

[34] https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf

[35] https://privacymark.org/

[36] https://www.jipdec.or.jp/protection_org/JIPDEC_AOP_CBPR_005.pdf

[37] Speech by Prime Minister Abe at the World Economic Forum Annual Meeting: Toward a New Era of "Hope-Driven Economy", 23 January 2019 <https://www.mofa.go.jp/ecm/ec/page4e_000973.html>.

with the important partners. For instance, Japan's relationship with the United States has featured economic dialogues and treaties since the 1970s[38], and a trade agreement was signed in October 2019 which entered into effect in January 2020[39]. With the same timeframe, Japan and the US signed a separate digital trade agreement[40]. There are important provisions pertaining to non-restriction on cross-border transfer of personal information (Art. 11 (1)), the prohibition of localised computer facilities (Art. 12), the maintenance of a legal framework for providing personal information with publishing information related to remedies and compliance requirements (Art. 15 (1)(2)), and the prohibition of transferring and accessing source code of software and to algorithms (Art. 17). In addition to these relationships, the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy, which began in 2010, holds annual meetings to consistent support the APEC CBPR system. A recent joint statement issued in September 2021 described that 'the CBPR system as a relevant mechanism to facilitate interoperability and create a globally useful and acceptable scheme for cross border data flows'[41].

2-2. Japan-EU/UK Relations

Regarding the EU, Japan and the EU collaborated since the 1991 Hague Declaration[42], through the Action Plan of the EU-Japan Cooperation in 2001[43] (see the Japan-EU Agreements below[44]). Since these commitments between two partners, Japan and the EU promoted the political and economic relations. According to the MOFA's survey, there are 6,537 Japanese corporations engaging business within the EU member states in 2017[45].

---

[38] For instance, there are several agreements such as 'Agreement between Japan and the United States of America concerning Cooperation on Anticompetitive Activities' (1999) and 'Agreement between Japan and the United States of America on Social Security' (2005).
[39] Trade Agreement between Japan and the United States <https://www.mofa.go.jp/mofaj/files/000527401.pdf>.
[40] Agreement between Japan and the United States of America concerning Digital Trade https://www.mofa.go.jp/mofaj/files/000527427.pdf>.
[41] Joint Statement on the 12th U.S.-Japan Policy Cooperation Dialogue on the Internet Economy, 18 November 2021<https://www.soumu.go.jp/main_content/000778689.pdf>.
[42] Joint Declaration on Relations between the European Community and its Member States and Japan, 18 July 1991. <https://eeas.europa.eu/archives/docs/japan/docs/joint_pol_decl_en.pdf>
[43] MOFA, An Action Plan for EU-Japan Cooperation. <https://www.mofa.go.jp/mofaj/area/eu/kodo_k_e.html>
[44] An overview of the Japan-EU relations is given by Takako Ueta, Japan's Relations with the EU in a Changing World, in Dimitri Vanoverbeke et. al. (eds) Developing EU-Japan Relations in a Changing Regional Context (Routledge 2018) 107.
[45] https://www.mofa.go.jp/mofaj/files/000112186.pdf

2002	Mutual Recognition Agreement
2003	Competition Agreement
2006	Agreement for Cooperation
2007	Partnership Agreement for the Join Implementation of the Broader Approach Activities in the Field of Fusion Energy Research
2008	Agreement on Cooperation and Mutual Administrative Assistance in Customs Matters
2009	Memorandum of Cooperation between the European Food Safety Authority and Food Safety Commission of Japan
2011	Agreement on Mutual Legal Assistance in Criminal Matters Agreement on Cooperation in Science and Technology
2013	Cooperation in the field of Disaster Management between the DG ECCHO, the European Commission and MILT
2015	Implementing arrangement between the European Commission and the Japan Society for the Promotion for Science for Japanese Researchers hosted by the European Research Council grantees in Europe

Two partners reached the Japan-EU Economic Partnership Agreement (EPA) with entry into force in February 2019. The Japan-EU Business Roundtable, initiating in 1999 with annual joint recommendation, contributed to policy recommendations including international data transfers. For instance, in April 2016, when both the PPC and the European Commission held the first dialogue, the Business Roundtable recommended that 'the Authorities of both the EU and Japan will start their work on establishing a framework as soon as possible, recognising the EU-US frameworks, so-called 'EU-US Privacy Shield''[46]. In result of the adequacy decision, the Roundtable 'welcomes the adoption of the Adequacy Decision allowing for the transfer of personal data between'[47].

According to the European Commission's factsheet, the EU exports over 80 billion euros' worth of goods and services to Japan annually, and there are more than 600,000 jobs in the EU related to these exports[48]. The Japan-EU EPA contains some important provisions regarding data protection and transfers of information, which reside in Chapter 8 title 'Trade in Services, Investment Liberalization and Electronic Commerce'. Although

[46] EU-Japan Business Round Table Joint Recommendations, 20 April 2016. https://www.eu-japan-brt.eu/sites/eu-japan-brt.eu/files/Part%20I%20recommendations%20endorsed%20FINAL.pdf
[47] EU-Japan Business Round Table Joint Recommendations, 15 May 2019. https://www.eu-japan-brt.eu/sites/eu-japan-brt.eu/files/2019_Part1-EN.pdf
[48] Commission, 'Factsheets about the agreement' 6 July 2017. https://trade.ec.europa.eu/doclib/docs/2017/july/tradoc_155684.pdf

the Japan-EU EPA is separate from the Japan-EU Mutual Adequacy Decision, the PPC participated in the Committee meeting on trade in services, investment liberalisation and electronic commerce[49].

Furthermore, Japan and the EU has been promoting cybersecurity cooperation through the EU-Japan Cyber Dialogue since 2014 as 'an upward trajectory'[50]. The Japan-EU ICT Policy Dialogue also contributed to the policy convergence such as the AI and 5G technologies. Most recently, in May 2022, Japan and the EU launched the 'Japan-EU Digital Partnership' with a statement that 'both sides recognise high privacy standards as an essential element of a human-centric approach to the opportunities and challenges of our digital age' [51].

Following Brexit, Japan was the first country to reach a trade agreement with the United Kingdom. The Japan- UK Comprehensive Economic Partnership Agreement (CEPA)[52], which entered into force in January2021. Art. 8.80(2) provides a general rule on privacy, stating that '[e]ach Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. Furthermore, each party should publish information regarding (a) how individuals can pursue remedies; and (b) business can comply with any legal requirements (Art. 8.80 (4)). Both Japan and the UK are encouraged 'to promote compatibility between these different regimes' of protecting personal information (Art. 8.80 (5)). Moreover, along the same line with the TPP, a specific provision was introduced forbidding the 'prohibit[tion] or restrict[tion of] the cross-border transfer of information by electronic means, including personal information' (Art. 8.84 (1)).

2-3. Data Localisation in Trade Agreements

Japan has a wide range of trade agreements and 21 existing EPAs/FTAs and related initiatives with 24 countries or regions. TPP 11 was the first major multilateral trade agreement related to personal information protection that Japan signed in January 2017. Chapter 14 of the TPP, titled 'Electric Commerce' contains several important articles relating to privacy. For instance, each party shall adopt or maintain a legal framework for

---

[49] Joint Minutes of the Second Meeting of the Committee on Trade in Services, Investment Liberalisation and Electronic Commerce under the Agreement between Japan and the European Union for an Economic Partnership, February 12, 2021 https://www.mofa.go.jp/mofaj/files/100198116.pdf

[50] George Christou and Yoko Nitta, EU-Japan Cybersecurity Cooperation, in Emil Kirchner and Hand Dorussen (eds) *EU-Japan Security Cooperation* (Routledge 2019) 159.

[51] https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/b530adc8-3af1-4d9f-af84-6f21af4067af/973dfec5/20220512_news_digital_group_original_02.pdf

[52] https://www.mofa.go.jp/files/100111408.pdf.

the protection of personal information in order to enhance consumer confidence in electronic commerce (Art. 14.8). At the same time, each party should publish information relating to the remedies for individuals and legal requirements for compliance by business (Art. 14.8 (4)). According to the TPP's data strategy, the cross-border transfer of personal information should be allowed to facilitate business (Art. 14.11). It also clarifies the prohibition of data localisation: the parties are prohibited from requiring the businesses to use or locate computing facilities in the party's own territory (Art. 14.13). Access to source code of software is also forbidden (Art. 14.17).

Japan signed RCEP in November 2020, along with ten ASEAN countries as well as Japan, China, South Korea, Australia and New Zealand, accounting for approximately one third of the world's population and the GDP. The RCEP has similar provisions in its general clauses relating to the protection of personal information such as adopting or maintaining a legal framework and publishing information of remedies and legal requirements for compliance (Art. 12.8)[53]. However, because China heavily influenced the RCEP, there is a remarkable departure from the TPP in that each party 'may have its own measures regarding the use or location of computing facilities' (Art.12.14 (1)). It is known that the Chinese Cybersecurity Act provides the critical information infrastructure operators to store personal information within mainland China[54]. Along with justification of data localisation, the RCEP allows each party to 'have its own regulatory requirements concerning the transfer of information' (Art. 12.15(1)). As such, the RCEP encourages parties to a dialogue on 'current and emerging issues, such as the treatment of digital products, source code, and cross-border data flow and the location of computing facilities in financial services' (Art. 12.16 (1)(b)). Thus, the RCEP is regarded as providing a relaxed standard of data protection that 'contain[s] more generous exceptions than … any of the bilateral agreements to date'[55].

Comparison of the TPP and the RCEP reveals a striking difference the data location regulation. While the TPP explicitly prohibits such regulation, the RCEP accommodates parties' data localisation measures. In Japan, under the Basic Act on Cybersecurity which provides the cybersecurity strategy, the Cybersecurity Policy for Critical Infrastructure Protection lists 14 categories of critical infrastructure operators that are not required to store data within Japan[56]. However, in the wake of the LINE data scandal, the Economic

---

[53] Chapter 12 of the RCEP is available at https://www.mofa.go.jp/files/100129114.pdf.

[54] *See* Daoli Huang, *Research on the Rule of Law of China's Cybersecurity* (Springer 2022) 58.

[55] Graham Greenleaf, 'Will Asia-Pacific Trade Agreements Collide with EU Adequacy and Asian Laws?' 167 *Privacy Laws & Business International Report* (2020) 21.

[56] Cybersecurity Strategic Headquarters, The Cybersecurity Policy for Critical Infrastructure Protection Annex1 <https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r2.pdf>.

Security Bill was submitted the Diet (the Japanese Parliament) in February 2022 in order to protect critical infrastructure by ex-ante review[57]. Emprical evidence presented in Martina Ferracane's 'The Costs of Data Protectionism'[58] details the costs of data protectionism to local companies in terms of jobs, productivity, and Gross Domestic Product (GDP). Additionally, a strict data policy is delineated, accompanied by the EU's GDPR costs for processing and transferring personal data. The study also assesses each country's data restrictive rules, pointing out that the strictest rule can be found in Russia, followed by China and Turkey. Japan is ranked 46 out of 64 countries in terms of data restrictiveness.

Each country's trade agreement reflects its data strategy. As will be analysed later, Japan promotes open and trustworthy data flow, while relying on multiple international frameworks such as the EU adequacy decision, the OECD Privacy Guidelines, and the APEC Privacy Cross-Border Rules. However, the choice of these international frameworks regarding different levels of privacy protection depends on political will. At least, in the context of data localisation, one can deduce based on the existing trade agreements that 'countries like Australia, Canada, Chile, Japan, Singapore, New Zealand, the United States, and the United Kingdom must collaborate on constructive alternatives to data localsation'[59]. The cost of data localisation should also be considered. Data isolation is often said to be costly and restrictive of e-commerce because most businesses abroad and local small and medium-seized enterprises (SMEs) cannot use cloud service providers as back-end infrastructure such as software as a service (SaaS), which stifles the talent of the employee and disadvantages remote workers[60]. However, at the same time, reasonable data harboring under the certain conditions within each jurisdiction may be benefitial, considering the risk involved in the export of sensitive personal data exported to the third country of lower level of protection[61].

---

[57] The Bill on Promotion to Ensure National Security by Taking Systematic Economic Policies is available the https://www.cas.go.jp/jp/houan/220225/siryou3.pdf (in Japanese).

[58] Martina F. Ferracane, 'The Cost of Data Protectionism' in Mira Burri (ed) *Big Data and Global Trade Law* (CUP 2021) 68.

[59] Nigel Cory and Luke Dascoli, 'Information Technology & Innovation Foundation, How Barriers to Cross-Border Are Spreading Globally, What and How to Address Them' (2021) 1 < https://itif.org/sites/default/files/2021-data-localization.pdf >.

[60] Anne Josephine Flanagan et. al., 'White Paper: A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy' (2020) 16-17. < https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf >

[61] For instance, the Court of Justice of the European Union stated in a data retention case that 'In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period'. Joined Cases C-203/15 and C-698/15, *Tele2 Sverig*, ECLI:EU:C:2016:970.

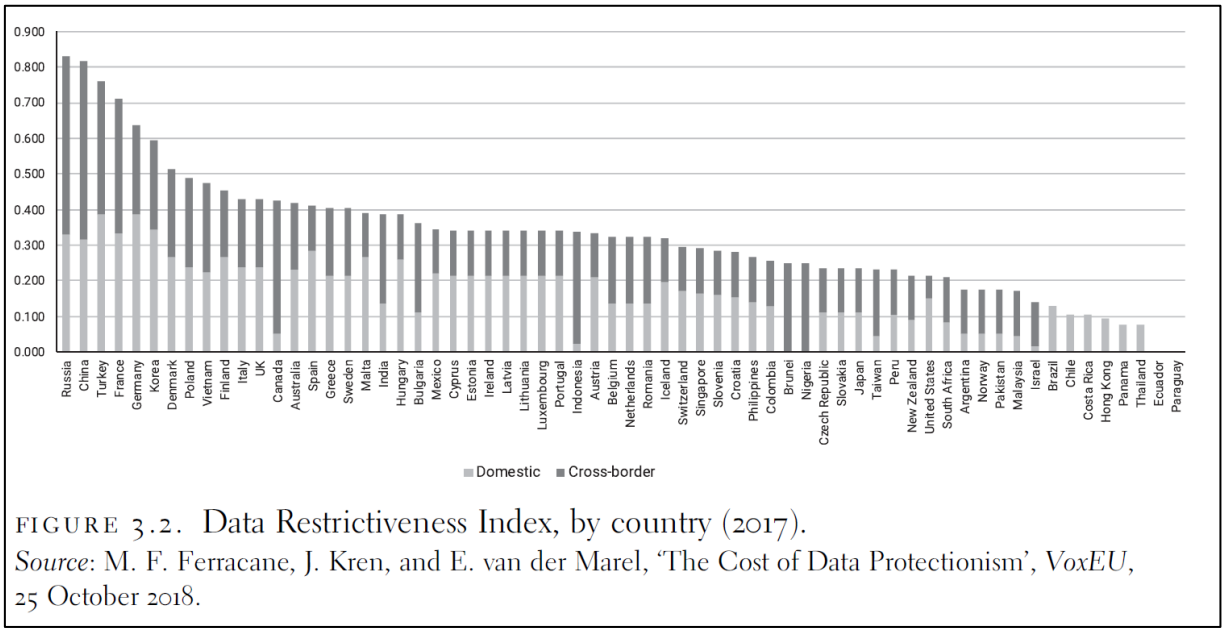

FIGURE 3.2. Data Restrictiveness Index, by country (2017).
Source: M. F. Ferracane, J. Kren, and E. van der Marel, 'The Cost of Data Protectionism', *VoxEU*, 25 October 2018.

2-4. Algorithmic Transparency in the New Digital Trade Agreements

The recent digital trade agreements include a provision regulating access to source code or algorithmic code. Japan has embraced several important trade agreements. On the one hand, the Japan-US and the Japan-UK trade agreements prohibit accessing source code in algorithm, on the other hand, the Japan-EU mutual adequacy decisions and the Japan-EU EPA are based on a preference for data protection as a fundamental right in Europe. Among these trade agreements, tension exists regarding algorithmic transparency among these trade agreements; namely, data subjects have a right to obtain meaningful information about the logic involved, as well as the significance and the envisaged consequences of data processing (Art. 13 (2)(f), Art. 14(2)(g) and Art. 15(1)(h)), while the Japan-US and the Japan-UK trade agreements prohibit access to source code of software or to algorithm. However, according to GDPR recital 63, '[t]hat right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject'. Thus, a question has been raised regarding the nature of algorithmic transparency in these trade agreements.

According to an explanation regarding the German court (Bundesgerichtshof)'s judgement under the Federal Data Protection Act of 2001, 'detailed information on the decision in the individual case was unnecessary and that a description of the abstract

design of the system was generally sufficient'[62]. While the Data Protection Directive Art. 12 (a) does not largely diverge from the GDPR's articles in terms of language, the GDPR has broader requirements. For instance, the GDPR requires the controller to provide 'meaningful information' instead of the 'knowledge of the logic involved' under the Data Protection Directive. Similarly, the GDPR includes 'the significance and the envisaged consequences', which were absent from in the Directive. The referenced case was decided before the implementation of the GDPR; hence, it is questionable whether this decision will automatically apply to similar cases post-GDPR including those in the context of trade agreements[63]. Thus, under the GDPR, it is unclear in what cases and to what extent the controller is required to provide information about the logic involved in automated decision making.

In Japan, the APPI has no equivalent provision regarding automated decision-making and its transparency. The Act on the Improvement of Transparency and Fairness of the Specific Digital Platform Operators of 2021 requires that digital platform operators disclose information relating to transaction conditions, which does not explicitly include source code nor algorithms. However, the Act delegates the compilation of disclosure lists by the Ministry of Economy, Trade, and Industry (METI), which entails listing the main issues involved in the decision of item ranking and search priority[64]. Despite the ambiguity of the legislation, newspaper articles reported that the Tokyo District Court in an antitrust case on 16 June 2022 ordered the restaurant ranking platform 'Taberogu' operated by Kakaku.com to disclose algorithm that the platform initially refused to do so due to its trade secret[65]. This case has exerted a huge implication on antitrust law, while a limited impact on data protection law since the plaintiff was a restaurant as a legal person, not a natural person for protecting personal data. However, if the same logic applied to an individual, regardless of trade secret, data subjects would request the

---

[62] Thomas Wischmeyer, 'Artificial Intelligence and Transparency' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer 2020) 83 (quoting BGH, Urteil vom 28. 1. 2014).

[63] DPD Art. 12(a) provides 'knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions', while GDRP Art. 13 (2)(f) states in a broader way 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.

[64] METI, 'Information available by the Act on the Improvement of Transparency and Fairness of the Specific Digital Platform Operators' (デジタルプラットフォーム取引透明化法によって知ることが出来る情報)
<https://www.meti.go.jp/policy/mono_info_service/digitalplatform/consumer.html>

[65] 'Taberogu Evaluation, Disclosure of Calculations' (食べログ評価掲載式開示), Mainichi Newspaper, 13 January 2022 (No details about the case is available including the case number). See also Financial Times, 'Japanese court ruling poised to make Big Tech open up on algorithms' 4 July 2022.

controller to disclose the meaningful logic involved in data processing information affecting him or her such as algorithm of scores or ranking.

This Tokyo District Court's judgment is also consistent with the Japan Fair Trade Commission (JFTC)'s approach on regulation of algorithmic transparency in the digital platform. JFTC's study group report indicates a stringent regulation is required in the case where an arbitrary algorithm ranking undermines the competition[66]. In addition, JFTC published 'Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc' in 2019 and later revised in 2022[67]. JFTC in its Guidelines invalidates the consent if such consent is obliged for no other alternative but to use the service for the sale of goods under the general consumer interests. In other words, data subjects' consent may be invalidated if the controller uses the algorithm in addition to its sale of goods and services without sufficient information to data subjects and their explicit consent[68]. Furthermore, the Act on Improving Transparency and Fairness of Digital Platforms was enacted in 2020 to enhance transparency in terms and condition. This Act requires the digital platform operators to disclose the information regarding the decisive factors on search ranking of the goods, though not specifically includes algorithm or source code (Art.5(2)(1)(ha))[69]. Apart from this Tokyo District Court case, there seems to be no other case that can definitively resolve the tension between the concepts of algorithmic transparency and trade secrets in Japan.

In sum, a controller may refuse to provide meaningful information about trade secrets or intellectual property, but it should be noted here that the EDPB's guidelines state that 'controllers cannot rely on the protection of their trade secrets as an excuse to deny access

---

66 JFTC Study Group on Competition Policy in Digital Market, 'Algorithms/ AI and Competition Policy'（「アルゴリズム／ＡＩと競争政策」） March 2021. pp.41-42. <https://www.jftc.go.jp/en/pressreleases/yearly-2021/March/210331004.pdf>

67 JFTC, 'Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc' 17 December 2019. <https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217DPconsumerGL.pdf>

68 JFTC Guidelines state that '… the said enterprise provides other services in addition to the sale of goods, no issue will normally arise if the digital platform operator acquires the personal information necessary for the provision of the additional services upon the express consent of the consumer who receives the additional services..' in note 13 and 'if consumers are compelled to consent to the use of personal information beyond the scope necessary to achieve the purpose of use because such consumers had no other alternative but to use the service for the sale of goods, the consent may be determined as made involuntarily' in note 18.

69 METI, 'Key Points of the Act on Improving Transparency and Fairness of Digital Platforms（TFDPA）' <https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/tfdpa.html>

or refuse to provide information to the data subject.'[70]. This is a new legal issue that has arisen amidst tension between the trade agreements and the GDPR which will bring an attention to the scope and extent of the information provision in relation to algorithm transparency. Neither legislation nor judicial review has yet resolved this contentious matter.

2-5. The Japan-EU Mutual Adequacy Decision and the EPA

The Japan-EU EPA signed in July 2018 'not only ha[s] economic significance but also have crucial political importance'[71]. In the process of negotiation between Japan and the EU over the EPA, '[t]he EU expressed its preliminary concerns and recalled that data protection standards or substance could not be negotiated via an FTA'[72]. The EU has been 'against bringing data protection to the trade talks. Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable'[73]. On the contrary, the Japanese government has advocated data governance including data privacy in the WTO forum rather than human rights instruments. Then-Prime Minister Shinzo Abe stated that '[l]et Osaka G20 set in train a new track for looking at data governance -- call it the Osaka Track -- under the roof of the WTO'[74]. In fact, the G20's Osaka Declaration in 2019 led by the Japanese government highlights that 'the importance of interface between trade and digital economy, … and reaffirm the importance of the Work Programme on electronic commerce at the WTO'[75]. During the EPA negotiation with the EU, 'Japan reiterated its interest in having provisions ensuring the free flow of data and the prohibition of data localisation requirements'[76]. Considering the distance between Japan's and the EU's initial stances on data protection, the Japanese PPC's initiation of an adequacy dialogue with the European Commission in April 2016 may not be coincidental

---

[70] Article 29 Data Protection Working Party (EDPB), 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 17' WP251rev.01, As last Revised and Adopted on 6 February 2018.

[71] Takako Ueta, 'Japan's relations with the EU in a changing world' in Dimitri Vanoverbeke et. al. (eds) *Developing EU-Japan Relations in a Changing Regional Context* 113 (Routledge 2018).

[72] Commission, 'Report of the 15th EU-Japan FTA/EPA negotiating round Brussels, 29 February - 4 March 2016' <https://trade.ec.europa.eu/doclib/html/154368.htm>.

[73] Viviane Reding, 'Speech: Towards a more dynamic transatlantic area of growth and investment' (SPEECH/13/867) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_13_867>.

[74] Speech by Prime Minister Abe at the World Economic Forum Annual Meeting: Toward a New Era of "Hope-Driven Economy", 23 January 2019. <https://www.mofa.go.jp/ecm/ec/page4e_000973.html>

[75] G20 Osaka Leaders Declaration, 28-29 June 2019. <https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html>.

[76] Commission, 'Report of the 18th EU-Japan FTA/EPA negotiating round Tokyo, Week of 3 April 2017' < https://trade.ec.europa.eu/doclib/html/155506.htm>.

given that it was one month later of the EPA negotiations where the EU warned not to discuss data protection on the trade agreement table.

After a series of negotiations between the EU and Japan, they signed the Japan-EU EPA and SPA in July 2018. Protection of personal data was separated from these two agreements since it forms a part of the fundamental rights agreement, which is of a different nature than the EPA and the SPA. However, both the EPA and the SPA inevitably include personal data protection provisions, raising a question as to the relationship between personal data protection as a fundamental right in the adequacy decision and personal data protection as a component of the EPA and the SPA.

Regarding the relationship between personal data protection as a fundamental right and as part of a commercial agreement, WTO's General Agreement on Trade in Services (GATS) provides the basic guiding principle. There exist possible scenarios where the GATS may theoretically step into privacy disputes. First, cross-border data flow may be recognised as 'trade in services' under GATS Art. I 2 (a) as it clearly includes cross-border trade[77]. Second, the GATS provides 'the Most-Favoured-Nation Treatment' which requires Members to accord the most favourable tariff and regulatory treatment given to the product of any one Member at the time of import or export of like products to all other Members (Art.2). Thus, a question may arise as to whether the special treatment of a particular third country in the name of adequacy can be justified under the GATS. In response to this question, the general exception will apply under GATS Art.14 (c) (ii) which provides for 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data', while prohibiting 'a means of arbitrary or unjustifiable discrimination'. This provision requires the necessity test in the WTO's jurisprudence. It seems that the EU's regulatory frameworks will meet this general exception clause without constituting 'a means of arbitrary or unjustifiable discrimination' based on the following reasons[78]. First, the EU's cross-border data flow regulation stems from a fundamental right to personal data protection as a necessary measure, even if it is transferred to a third country. Second, cross-border data flow regulation is permissible and authorised under existing international instruments such as the OECD Privacy

---

[77] WT/DS204/R, Mexico - Measures Affecting Telecommunications Services - Report of the Panel, 2 April 2004 ('…*the services at issue, in which United States suppliers link their networks at the border with those of Mexican suppliers for termination within Mexico, without United States' suppliers operating, or being present in some way, in Mexico, are services which are supplied cross-border within the meaning of Article I:2(a) of the GATS*' para7.45).

[78] There are possible objections in this statement, for instance, 'the system by which the Commission white-lists countries may be irreconcilable with GATS'(Jan Xavier Dhont, 'Schrems II. The EU adequacy regime in existential crisis?' (2019) 26 Maastricht Journal of European and Comparative Law 597, 599). However, this issue is the beyond the scope of this paper.

Guidelines and the Convention 108+ as well as many national legislations. And third, as the GDPR prepared for several alternative options for transferring personal data other than the adequacy decision, the adequacy scheme may not constitute an arbitrary or unjustifiable discriminatory regulation.

To echo this scenario, the trade agreements involving Japan that entered into force include a similar provision[79]. The EU-Japan EPA includes 'General exceptions' clauses in trade in services (Art.8.3). emphasizing the need to protect privacy of individuals (Art. 8.3, 2(c)(ii)). This endorses the GATS's framework and proves consistency with the necessity test of protecting privacy of an individual. Under such circumstances, the EU-Japan EPA will not be used an excuse of exemption from rights and obligations under the data protection laws and the adequacy decision. In fact, in case of the EU-Japan relationship, data protection was not an issue of exception in the EPA, rather both parties viewed it as a positive matter toward a high level of protection. In other words, '[p]rivacy and personal data protection were discussed not merely as an exception, but as a positive obligation counterbalancing the parties' possible commitments to cross-border information flows'[80].

2-6. The Japan-EU Mutual Adequacy Decision and the SPA

Along with the EPA, the Strategic Partnership Agreement (SPA) promotes cooperation on matters of mutual interest in a wide range of areas from personal data protection, cyber-issues, and counter-terrorism to environment, energy, and health[81]. The SPA establishes 'a high level of protection of personal data.' (Art. 39), focusing on the data protection in the context of counter-terrorism (Art. 8) and passenger name record (PNR) (Art. 37). This may reflect that the Japan received the partial adequacy decision in the private commercial sector only, so that commitment to the public sector data protection was manifested to ensure a high level of protection of personal data in promoting cooperation of counter-terrorism and passenger name record. As the SPA is recognised to some extent as introducing 'new horizons of EU–Japan security

---

[79] There is one Japanese article regarding the relationship between the WTO and EU adequacy decision. Mariko Kunimi, 'An Examination concerning personal data protection system from the aspect of adequacy requirement of EU personal data protection directive/regulation and WTO agreement' (2014) 63 InfoCom Review 26 (國見真理子「EU 個人データ保護指令/ 規則と WTO 協定との関係を中心とした個人情報保護制度に関する一考察」).

[80] Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade' (2020) 10 International Data Privacy Law 201, 208.

[81] Ministry of Foreign Affairs of Japan, 'Japan-EU Strategic Partnership Agreement (SPA)' <https://www.mofa.go.jp/files/000381944.pdf>.

cooperation'[82] including the defence capability development involving new technologies such as AI based EU and Japan Partnership on Sustainable Connectivity and Quality Infrastructure.

Regarding the security relationship as a part of the EU-Japan SPA, the issue is more complicated by the fact that the adequacy decision only covers the private sector. While the EU-Japan cooperation in the private sector services will benefit from the adequacy decision, public sector mutual assistance should rely on other tools for transferring personal data from the EU. For instance, the SPA includes the topic on the PNR for the purpose of detecting imported goods linked to terrorism and illegal drugs. The EU and Japan initiated a dialogue on the EU-Japan PNR Agreement in February 2020[83]. The Japan Customs Office collects 35 items of personal data from airline companies 72 hours before departure from foreign or Japanese airports. The EDPS issued an opinion, stating that 'the envisaged Agreement must include appropriate legally binding and enforceable safeguards' [84]. Compared with the EU-Canada PNR agreement [85], there was no supervisory authority regarding the Customs Office which is in charge of PNR until April 2022 when the amended APPI brought the PPC's expanded power to the public sector. According to Tokyo Custom's normal document management rule, the PNR data are retained for seven years[86], which is two-year longer than Canada.

With regard to police cooperation, both Europol and the National Police Agency of Japan issued a 'Working Agreement on establishing cooperative relations between the National Police Agency of Japan and the European Union Agency for Law Enforcement Cooperation' [87] in December 2018. However, Article 8(3) of Working Agreement provides that 'this agreement does not provide for the legal basis for the transfer of personal data' with an exception clause under Art. 25 (5) or 25 (6) of the Europol Regulation.

The SPA also encompasses more difficult areas. For instance, regarding the Japan-

---

[82] Emil J. Kirchner & Han Dorussen, 'New Horizons in EU–Japan Security Cooperation' (2021) 19 Asia Europe Journal 27.

[83] Council, 'Decision authorising the opening of negotiations with Japan for an agreement between the European Union and Japan on the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and serious transnational crime' (5378/20).

[84] EDPS, 'Opinion 6/2019 on the negotiating mandate of an Agreement between the EU and Japan for the transfer and use of Passenger Name Record data' 25 October 2019, 7.

[85] CJEU, Opinion 1/15, Opinion pursuant to Article 218(11) TFEU, ECLI:EU:C:2017:592.

[86] Ministry of Finance, Tokyo Customs, Standard of Retention Period of Normal Documents <https://www.mof.go.jp/application-contact/procedure/disclosure_etc/disclosure/kanrikisoku/102tokyo20210226.pdf> (in Japanese)

[87] <https://www.europol.europa.eu/agreements/working-arrangement-establishing-cooperative-relations-between-national-police-agency-of-japan-and-european-union-agency-for-law>

EU Mutual Legal Assistance Agreement, 'the conclusion of the Agreement has not contributed and will unlikely contribute to the EU promotion of its values in Japan, notably influencing the Japanese position on capital punishment'[88].

2-7. Summary: Beyond Data Nationalism

Protection of personal data has been debated through several channels from the human rights forum to commercial negotiations. Japan and the EU shares a basic framework on data protection, in particular the Japanese amendments in 2020 and 2021. While the Japan-EU EPA and SPA include several provisions regarding protecting personal data, the adequacy decision should, in principle, prevail over these agreements as the human rights standard cannot be watered down by other motivations. This was endorsed by the GATS understanding which was incorporated into the EPA agreement. There still exist some areas where the EU and Japan stand a certain distance apart regarding public sector cooperation such as mutual legal assistance due to the existence of capital punishment in Japan.

Nevertheless, the data protection convergence between 'the EU acting as a data convergence actor'[89] and Japan serving as a data flow promoter is a success story. Moreover, '[t]he high level of regulatory convergence between data privacy laws in Japan and the EU likely mitigates the risk of a trade law dispute over data privacy measures'[90]. At the same time, implementation of such data convergence has just begun, so upcoming periodical reviews will reinforce, or should even void if there were a significant divergence in the mutual adequacy decision in the future. However, the history shows that the EU and Japan have been strengthening their relationship from 1991 to 2022 without any significant divergence.

3. Towards Global and Regional Convergence

3-1. Data Free Flow with Trust (DFFT) in the globe

---

[88] Anne Weyembergh & Irene Wieczorek, 'Norm Diffusion as a Tool to Uphold and Promote EU Values and Interest: A Case Study on the EU Japan Mutual Legal Assistance Agreement' 11 New journal of European Criminal Law (2020) 439, 465.

[89] Fahey, Elaine and Mancini, Isabella, 'The EU as an Intentional or Accidental Convergence Actor? Learning from the EU-Japan Data Adequacy Negotiations' (May 20, 2020) International Trade Law and Regulation 2020 Volume 2 <https://ssrn.com/abstract=3606087>.

[90] Marija Bartl & Kristina Irion, 'The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun' (October 25, 2017). Available at SSRN: https://ssrn.com/abstract=3099390.

Japan has an ambition of converging data flow and protection frameworks under the 'Data Free Flow with Trust (DFFT)' initiative. 23 January 2019 marks a special day for the Japan-EU mutual adequacy decision. On that day at the Davos World Economic Forum, the world leaders including Japan revealed their data strategies. Then German Chancellor spoke in the Forum with under categories in the digital orientation[91]. One is the US approach with data in the hands of private stakeholders. Another is the Chinese approach with data extensively accessed by the government. On the contrary, the EU approach as the third way is based on 'civilizational developments' with a certain degree of privacy with the GDPR.

After Chancellor Merkel's speech, then-Prime Minister Abe spoke that '[t]he regime we must build is one for D.F.F.T., Data Free Flow with Trust' at the Forum'[92]. Japan has been promoting the 'Data Free Flow with Trust' initiative since then. In 2019, the G20 Osaka Leaders' Declaration endorsed DFFT, declaring that 'data free flow with trust will harness the opportunities of the digital economy'[93]. This Declaration clearly recognises the privacy and data protection, stating that '[c]ross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security'.

The G7 continues to promote DFFT in 2021 with the G7 Digital Trade Principles, namely, '[p]ersonal data must be protected by high enforceable standards, including when it is transferred across borders. … We will cooperate to explore commonalities in our regulatory approaches and promote interoperability between G7 members'[94]. A G7 Roadmap for Cooperation on Data Free Flow with Trust was later published in the UK host in 2021[95]. The Roadmap sets out the agenda items of 1) data localisation, 2) regulatory cooperation, 3) government access to data, and 4) data sharing for priority sectors. Japan will host the G7 Summit with 'the intention of the Japanese G7 Presidency

---

[91] Bundesregierung, 'Speech by Federal Chancellor Angela Merkel at the 49th World Economic Forum Annual Meeting in Davos on 23 January 2019'. < https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-angela-merkel-at-the-49th-world-economic-forum-annual-meeting-in-davos-on-23-january-2019-1574188 >

[92] MOFA, Speech by Prime Minister Abe at the World Economic Forum Annual Meeting, 23 January 2019 < https://www.mofa.go.jp/ecm/ec/page4e_000973.html >

[93] G20 Osaka's Leaders Declaration, 28-29 June 2019. <https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html>

[94] G7 Trade Ministers' Digital Trade Principles < https://www.meti.go.jp/press/2021/10/20211022008/20211022008-3.pdf >.

[95] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf >

in 2023 to continue work … on online safety and DFFT, including promoting regulatory cooperation for DFFT, in particular through round table discussions of data protection and privacy authorities'[96].

3-2. DFFT in Japan

In Japan, the Digital Agency, which was newly established in September 2021, published a data strategy report, which mentions the DFFT's a global framework while respecting each nation's political., economic, and social background[97]. Aiming at the 2023 G7, the Agency is also targeting 1) data localisation, 2) government access to private date through the OECD and the World Economic Forum, and 3) participation to the workshops in the common interest areas[98].

Additionally, Ministry of Economy, Trade, and Industry (METI) also held meetings about DFFT from November 2021 to February 2022 and produced a final report[99]. In this final report, the METI suggested the following points.

1) Transparency: It is important to ensure transparency of laws and requirements pertaining to transfer regulations which are often vague.
2) Technology and Standardization: It is necessary for the multi-stakeholders to cooperate regarding technical privacy and security practices when transferring data.
3) Interoperability: Considering the obstacles involved in corporations' data flow due to the lack of clarity regarding protection standards it is necessary to seek interoperability-based policy options.
4) Complementarity: Realisation of DFFT will be complemented by and harmonized with the existing commerce rules and general principles.
5) Implementation: DFFT should be implemented through policies such as reporting system via national legislative amendments and review of the efforts of each nation

Trust building is also an issue in the Japanese stakeholders. For instance, Trusted Web

---

[96] Ministerial Declaration G7 Digital Ministers' meeting, 11 May 2022, para 38. <https://www.soumu.go.jp/main_content/000813431.pdf>

[97] Digital Agency, Comprehensive Data Strategy, June 2021, p.50. < https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf >.

[98] Digital Agency, 'Proposal on the Comprehensive Strategy on Data in the Future' October 2021 (包括的データ戦略の今後の進め方（案）). <https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/7fd300a0-0bd3-44cf-89da-d6721381fa11/20211025_meeting_data_strategy_wg_01.pdf>

[99] <ttps://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2.pdf>

Promotion Council under the Cabinet Secretariate published 'Trusted Web White Paper ver.1.0' in March 2021[100]. This White Paper aims to ensure the safety in the digital platform to meet the users' expectation from a technical perspective. The basic idea is to promote authentication for data flow in the P2P systems. Verifiable credentials are given for the trusted senders and receivers for data exchanges with traceable functions. The government supports a trust anchor as the independent third party issuing verifiable credentials for ensuring the entire trusted data flow. Such trusted data flow will be appliable in the digital advertising and fact checking in the social media and detection of malicious entities[101]. Ministry of Internal Affairs and Communications also supported the e-seal as trusted digital signatures without any possibility to tampering the dates and the individual[102].

PPC also published 'Global Strategy' on March 2022, stating its will that '[l]ooking ahead for the Japan's G7 Presidency in 2023, the PPC Japan will deepen cooperation with other authorities through presentation and dialogues on the importance of DFFT in the international frameworks such as the Global Privacy Assembly (GPA), the Asia Pacific Privacy Authorities (APPA) and the G7, etc. aiming to further promote DFFT'[103]. In this statement, the PPC clearly mentions 'the global certification system' as 'a core of PPC's global strategy' with an aim of allowing 'different frameworks such as GDPR or APEC CBPR to coexist, and be inclusive, not exclusive'. At the same time, the PPC recognises 'emerging risks such as unlimited government access and data localization which may threaten DFFT'. It is likely the main topic of the coming years for the PPC to realise this 'global corporate certification system' in practice.

As abovementioned documents have illustrated, the DFFT initiative is still in its infancy with a big political ideal. Furthermore, there is a controversy in the Japanese DFFT that calls for the intervention of the WTO as a dispute resolution agency in the context of cross-border data flow. As previously investigated, '[i]t is not clear why shifting discussions back to a WTO forum will have any effect in relation to data privacy, although it might in relation to IP and cybersecurity'[104]. The association of data privacy

---

[100] Trusted Web Promotion Council, 'White Paper on Trusted Web ver. 1.0' 12 March 2021. (in Japanese) <https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/documents_210331-2.pdf>

[101] Demonstrations are available at https://github.com/TrustedWebPromotionCouncil/.

[102] Working Group on Examining Trusted Services, Final Report by the Working Group on Examining Trusted Services, Research Meeting on Platform Services, November 2019 (in Japanese) <https://www.soumu.go.jp/main_content/000657098.pdf>.

[103] PPC, 'Global Strategy of the Personal Information Protection Commission' 30 March 2022 <https://www.ppc.go.jp/files/pdf/global_strategy.pdf>.

[104] Graham Greenleaf, 'G20 Makes Declaration of 'Data Free Flow With Trust': Support and Dissent' (2019) 160 Privacy Laws & Business International Report 18.

in the cross-border data flow with the WTO will result in the treatment of data privacy as an economic and commercial product rather than a human rights issue. The Japanese approach may be found at the highest ideal of human-centric philosophy in the digital age. The Japan's ambition of realising the DFFT may depend on a consensus on a human-centric approach to the digital economy and how such consensus may be implemented in practice. With these goals, Japan aims to lead the DFFT discussion in 2023 as the host of the G7 meeting[105].

3-3. Summary

Convergence is a matter of degree in the political, legal, and economic dimensions. In the political dimension, both the G7 and the G20, in addition to the bilateral the Japan-EU and Japan-US relations, have endorsed DFFT. In the legal aspect, Japan and the EU mutually authorizes data flow based on reciprocity in the private sectors by respecting the essence of data protection right. In the economic area, Japan has already reached agreements with the EU, the UK and the US.

Regarding value convergence, not all values are shared in common between the EU and Japan. Apart from with respect to the commercial private sector, Japan has not yet received an adequacy decision from the EU. However, there are several public sector agreements such as on police cooperation to supplement these gaps. In order to address the emerging technologies, it is not coincidental that both Japan and the EU use the same terminology to describe their 'human-centric' approach to their AI regulatory frameworks. In Japan, the Social Principles on AI embrace the basic philosophy as human-centered data processing[106]. The EU's proposed AI Act also founded in the human-centric notion with the strategy of placing human at the centre of AI developments[107]. Digital developments and data protection in the age of global data flow will be based on these common values.

---

[105] See also Digital Agency, Priority Policy Program for Realizing Digital Society- Summary - < https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/0f321c23-517f-439e-9076-5804f0a24b59/20211224_en_priority_policy_program_02.pdf>

[106] Cabinet Secretariat, 'Social Principles on Human-Centric AI 'March 2019. <https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf>

[107] Commission, 'Communication: Building Trust in Human Centric Artificial Intelligence' COM(2019)168).