EU-JAPAN MUTUAL ADEQUACY DECISION

By Hiroshi Miyashita
Associate Professor, LL.D., Chuo University, Tokyo, Japan.

I- MUTUALLY BENEFICIAL DATA PROTECTION

Both the European Commission and Japanese Personal Information Protection Commission (PPC) publicised their adequacy decisions on 23 January 2019. While the EU gave adequacy decision to the first third country under the General Data Protection Regulation, Regulation (EU) 2016/679 (GDPR) and the first Asian country, Japan issued its first equivalency decision under the Act on the Protection of Personal Information (APPI).

It is not easy to bridge two legal systems, regardless of its different cultures and social norms. However, this has been achieved through the mutual adequacy decisions, thus opening a new chapter of data protection law throughout the world. The mutual adequacy does not mean that the EU and Japan have completely integrated their data protection laws and practices, rather, the two have agreed to live together remotely while trusting each other to protect personal data. Indeed, data transfer regulations can work as tools to connect different systems through trust and future assurances to cooperate for progress.

Unless they do not have any economic, cultural, or social relationships with the EU, no third country or international organisation can ignore the EU’s adequacy framework. The ‘essence’ of data protection in the EU is partly and externally guaranteed through the adequacy framework. As the ‘Brussels effect’ stands for the EU influences posed to third countries, the effects of the adequacy framework from within the EU also have external global effects. At the same time, the adequacy scheme may become a form of ‘carrot and stick’, thus rewarding third countries (such as Japan). However, this threatens countries outside the EU in matters related to trade (e.g. the EU-US Safe Harbour decision, which was later invalidated by the Court of Justice of the European Union (CJEU)).

This article discusses the mutual adequacy decisions and assignments consequently given to Japan for the next step. For one thing, it raises potential risks related to the partial adequacy decision, which only covers the private sector and may therefore be revised by the Japanese legislators in the near future. In sum, the mutual adequacy decision between the EU and Japan was a forward-looking and mutually beneficial political choice that will shape the ‘essence’ of data protection philosophy for decades.

II- EU ADEQUACY DECISION

A- DATA TRANSFER REGULATIONS

As the OECD Privacy Guidelines in 1980 explains ‘transborder flows of personal data’ are sources of a major concern; the initial agreement was ‘to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data’. However, European nations became aware that existing regulatory instruments were ‘not necessarily adequate for all the new and specific concerns involved’. In regard to drafting the adequacy framework, data transfer regulations stemmed from ‘a Europe of merchants rather than a Europe of human rights’ in the early stage. Despite the potential trade conflict, the EU approach to data transfer regulations...
was nevertheless shaped and later reinforced by a human rights concept. In Schrems case, the Court of Justice of the European Union justified the adequacy framework for the third country to ensure ‘a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order’

According to Professor Christopher Kuner, cross-border data flow regulations come in two forms; namely, this includes the geographically-based approach, which is focused on the location where the data are to be transferred, and the organisationally-based approach, which is focused on the organisations that received the data abroad. The EU chose the geographically-based approach in regard to adequacy decisions that apply to third countries or international organisations. The Asia-Pacific Economic Cooperation (APEC) has chosen the organisationally-based approach through its accountability principle. While the two approaches are not mutually exclusive, it should be noted that they may still be incompatible in some regards. For instance, a third country may have an adequate level of protection through its personal data legislations, but the residing organisations may not comply with such level of protection, and vice versa. The adequacy framework therefore exerts a strong influence on the third country, which is not the only way to export the EU's data protection philosophy to the the nations. The GDPR prepared for several venues by ensuring the level of protection when transferring personal data from the EU. For instance, it established the Binding Corporate Rules (BCRs), standard data protection clauses, codes of conduct and certifications (Art. 46 & 47). In one example, the leading Japanese e-Commerce company, Rakuten, obtained BCRs from the Luxembourg data protection authority before the GDPR entered into effect

B- ADEQUACY REVIEW AND PROCESS

The adequacy framework came in 1995 EU Data Protection Directive, which provides that the transfer to a third country of personal data may take place only if the third country in question ensures ‘an adequate level of protection’ (Art. 25 (1)). The ‘an adequate level of protection’ phrase is also used in the GDPR (Art.45(1)), but with additional clarifications regarding the assessment criteria. The Policy Directive 2016/680 also included similar provisions related to the the adequacy decision (Art. 36(1)). The Court of Justice elaborated the concept of adequacy as a level of protection for fundamental rights and freedoms which is ‘essentially equivalent’ rather than ‘identical’ to the EU legal order.

According to the Art. 45 (2) of the GDPR, the following three criteria are taken into account for the European Commission to assess adequacy decisions. In short, these criteria are

i) The rule of law, respect for human rights and fundamental freedoms, relevant legislation as well as effective and enforceable data subject rights and effective administrative and judicial redress

ii) The existence and effective function of independent supervisory authorities

iii) International commitments (such as accession to the Council of Europe’s Convention 108 (recital 105))

In addition to the text of the GDPR, the Article 29 Data Protection Working Party, since replaced by the European Data Protection Board (EDPB), adopted a paper on ‘Adequacy Referential’, which was originally published as a Working Document on transfers of personal data to the third countries (WP12). In this paper, the assessment details are categorised into two components, including (i) content principles (i.e., concepts, grounds for lawful and fair processing for legitimate purposes, the purpose limitation principle, the data quality and proportionality principle, data retention principle, the security and confidentiality principle, the transparency principle, the right of access, rectification, erasure and objection, restrictions on onward transfers, and additional contentment principles such as special categories of data, direct marketing and automated decision making and profiling) and (ii) procedural and enforcement mechanism (i.e., competent independent supervisory authority, the data protection system which ensures a good level of compliance, accountability and the data protection system providing support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms). After the Schrems case, the adequacy criteria also addressed essential guarantees for law enforcement and national security access in order to limit interferences to fundamental rights in...
third countries. For that reason, the following points also require consideration in the context of government access to private data; i) processing should be based on clear, precise and accessible rules (legal basis), ii) necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated, iii) the processing has to be subject to independent oversight, and iv) effective remedies need to be available to the individuals. In this regard, the EU adequacy set ‘the global data protection bar at a high level’.

The process of adequacy decision process is ‘long and tortuous’, with some review cases taking a few years to complete. In case of Japan, it took approximately two year and ten months after the first dialogue between the PPC and the European Commission in April 2016. Yet, a careful review is required for third countries due to the different legal regimes, backgrounds, and practices. Furthermore, the limited availability of open sources in English prompts experts including a local expert in the third country to prepare for the assessment reports for the European Commission during the adequacy review process. The adequacy decisions process involves the following specific steps:

- A proposal from the European Commission
- An opinion of the European Data Protection Board
- An approval from representatives of EU countries
- Adoption of the decision by the European Commission

Prior to the GDPR’s application, the European Commission listed 11 countries (i.e., Andorra, Argentina, Canada (commercial sector), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay) in addition to the EU-US Privacy Shield as providing adequate protections. It is considered ‘politically provocative or at least discriminatory’ if the European Commission prepares a black-list not ensuring adequate levels of protection.

In January 2017, the European Commission publicised an adequacy strategy with four following criteria; i) the extent of the EU’s commercial relations, ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties, iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region, and iv) the overall political relationship. The Commission, then recognising ‘a diverse range of privacy systems, representing different legal traditions, as being adequate’ and ‘will actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017’.

C- JAPAN’S PREPARATION FOR ADEQUACY REVIEW

Although the original APPI was enacted in 2003 and took full effect in April 2005, there was almost no possibility to obtain adequacy from the EU. This was mainly because no independent supervisory authority existed. Furthermore, the original APPI reflected the 1980 OECD Privacy Guidelines instead of the EU Data Protection Directive. At least in the Diet, there were no substantive discussions on adequacy until the Consumer Affairs Agency published a study report on EU adequacy in March 2012.

References:
12 Case C-362/14, Schrems, para 88 [...] limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.
19 Id.
20 The House of Representatives, Cabinet Committee, The 181st Diet, 7 November 2012, Chief Cabinet Secretary, Osamu Fujimura’s Statement. During the preparation of the original draft of APPI, the government responded that it explained the effectiveness of the Japanese self-regulation to the EU. House of Representatives, Plenary Session, 145th Diet, 13 April 1999, Minister of Foreign Affairs Masahiko Komura’s statement. The Consumer Affairs Agency’s study report on the international standards regarding the personal information protection system (March 2012) is available at https://www.ppc.go.jp/files/pdf/personal_report_2403caa.pdf (in Japanese).
The Japanese government later publicised a plan to request the European Commission to initiate an adequacy assessment in April 2015 when the amendments bill of the APPI was submitted to the Diet (Japanese Parliament). Then-Minister of State Shunichi Yamaguchi announced in the Diet that 'the government, in the relation with the EU, will make progress toward obtaining adequacy finding from the EU after passing the amendments bill in order to improve the business environment for the corporations within the EU'\(^2\). Japanese industries then pushed the Japanese government to request adequacy findings in order to realise a business environment entailing free flow of personal data between the EU and Japan\(^2\).

The Japanese strategy for adequacy was to seek a positive decision solely for the commercial private sector in order to promote industrial data flows. Furthermore, the structure of the Japanese legal regime meant that the European Commission could assess only the private sector and exclude the public sector not being supervised by an independent authority. Japanese data protection laws are divided: the APPI which covers the private sector, and 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, etc. (APPI-IAA) which cover the public sector. Laws that apply to the public sector are supervised by the Ministry of Internal Affairs and Communications, while the Japanese independent authority known as PPC has jurisdiction over the APPI, thus overseeing the private sector (with some exceptions such as non-identifiable processing information and national identification numbers). As such, PPC has no authority to supervise law enforcement and national security agencies in Japan. Before the PPC was established in 2016, the competent Ministry system was adopted through the APPI, under which each Ministry could issue instructions, recommendations and orders to each business field.

Prior to the official request for an adequacy review, the Japanese government was aware of some missing elements, including a lack of an independent supervisory authority, sensitive data, small business exemptions, data transfer restriction, and the need to clarify the right to access\(^3\). In addition, Professor Graham Greenleaf extensively examined the Japanese law and practice, concluding that there was 'a lack of evidence that the legislation is effective, which could be remedied somewhat by Ministries gathering and publishing more detailed data on compliance, enforcement, breaches and remedies'\(^4\). These improvements were incorporated into APPI amendments in 2015. Most importantly, the PPC was thereby established as an independent authority consisting of one chairperson and eight commissioners with diverse backgrounds; these individuals were tasked with supervising the private sector. The amended APPI also stipulated that sensitive data called as special-care required personal information, in which race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime are listed. Furthermore, small enterprise exemptions were abolished, by which even the small business handling personal data from 5,000 individuals or less are now required to comply with the APPI. Finally, as the original APPI did not contain an article regarding data transfer, a similar provision to the EU was introduced as 'equivalent' level of protection of personal data (Art. 24)\(^5\).

The new APPI entered into effect into May 2017, which then was officially ready to proceed with an adequacy review from the European Commission. Yet, during the PPC’s dialogue with the European Commission, the PPC realised that some areas in the APPI needed improvement. In April 2017, the PPC suddenly publicised a draft Guidelines on handling personal data transferred from the EU under the adequacy finding to be followed by public consultation. The draft Guidelines included the

\(^{21}\) House of Representatives, Plenary Session, The 189th Diet, 23 April 2015, Minister Shunichi Yamaguchi’s statement.

\(^{22}\) The 11th annual meeting of the EU-Japan Business Round Table, Recommendations to the EU and Japan from Multilateral and bilateral trade & investment, and regulatory cooperation, 6–7 July 2009. ‘...the government of Japan should request the European Commission to launch the adequacy-finding procedure on the basis of Article 25(6) of Directive 95/46/EC’.


\(^{24}\) European Commission, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments- BS Japan, 2010 (Graham Greenleaf).

\(^{25}\) 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; hereinafter the same in this Article) 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 recognised 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), 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.

https://blogdroiteuropeen.com
The EU-Japan Relationship

EU-JAPAN MUTUAL ADEQUACY DECISION

five following points. i) Special care-required personal information now also includes data concerning a natural person’s sex life or sexual orientation and trade-union membership, which are not explicitly mentioned in the APPI. ii) Retained personal data is protected irrespective of the period in which it is set to be deleted, though the Cabinet Order excludes personal data retained for less than six months. iii) The business operator must confirm and record the purpose for which personal data is received from the EU, in addition to items to be confirmed and recorded under the APPI. iv) As to the restriction on data transfers to a third party in a foreign country, a third party must obtain consent from data subjects in advance, or the third party’s country must meet the level of protection equivalent to that in Japan, and the third party then implements appropriate and reasonable measures such as contract or binding arrangements within a company group. v) Anonymously processed information should make the de-identification of the individual irreversible for anyone, though there are only requirements of non-identifiable and non-restorable information under the APPI. Among these five elements, the data transfer restrictions are notably stricter than the original PPC’s Guidelines, which allows the company to use the APEC Cross-Border Privacy Rules to fit the e-commerce scheme in this region.

The draft Guidelines were later changed after the public consultation its name into ‘Supplementary Rules’, which by itself insists ‘binding’ nature. However, there were still doubts about this binding nature due to the lack of a direct legal grounds under the APPI in addition to the absence of any endorsements via the democratic process of the Diet. Furthermore, the Supplementary Rules discriminate between the domestic personal data and the one transferred from the EU in that the domestic Japanese LGBT data or labour union data is not treated as sensitive data while the only the data from the EU will be protected as such. Enforcement of these ‘Supplementary Rules’ by PPC would inevitably raise constitutional questions of due process, equal protection, and legislative delegation.

With these legislative amendments, as an international commitment, Japan became a member of the International Conference of Data Protection and Privacy Commissioners’ (now the Global Privacy Assembly) in 2017 (which was initially rejected in 2016 because the amended APPI had not been fully implemented at that time). Japan has also been attending the Council of Europe’s data protection meetings as an observer, but has not yet accessed the Convention 108+.

D- THE COMMISSION’S DECISION

The European Commission finally issued an adequacy decision on 23 January 2019 after extensive and objective examination of the APPI and the related Japanese laws and practices concerned with personal data protection. The Commission’s adequacy decision of Japan covered the APPI as complemented by the Supplementary Rules set out in Annex I, together with the official representations, assurances and commitments contained in Annex II. Annex II regarding government access is the official documents singed by several Ministries and Agencies with the detail descriptions of the Japanese legal framework.

On 23 January 2019, the European Commission and PPC issued a joint statement which highlighted ‘the world’s largest area of safe data transfers’ with ‘the high degree of convergence between the two systems’. The Japan Business Council in Europe welcomed the adequacy decision, with the statement that ‘international trade and data protection rules should and can be developed in tandem to stimulate investment, innovation and partnerships in the data economy’.

27 Art.6 of the APPI provides that ‘[t]he government shall ... take necessary legislative and other action’, which does not automatically lead a binding nature of related Guidelines. See Graham Greenleaf, Japan’s proposed EU adequacy assessment: substantive issues and procedural hurdles, Privacy Laws & Business International Report Issue 154 (2018) p.8 (quoting Professor Shizuo Fujiwara’s article of questioning the binding nature of the Supplementary Rules). Another scholar also noted regarding the Supplementary Rules that it is impossible to recognise the legal bindingness in the guidelines from the principle of administration by law (prinzip der gesetzmaßigen Verwaltung), which definitely stipulates a legislation in case of infringing individual rights by administrative organs. Mayu Terada, Comparison and Lessons of the Personal Information Protection Regimes in the EU and Japan, Hikakuho Kenkyu vol.81 (2019) p. 181-182 (in Japanese).
28 Japan formally ratified the Budapest Convention on Cybercrime of the Council of Europe (CETS No.185) which entered into effect on 1 November 2012.
The data transfer agreement has remained one of the highest political commitments between the EU and Japan. In July 2018, both leaders from the EU and Japan welcomed ‘the talks paving the way for a simultaneous finding of an adequate level of protection by Japan and the EU’[32]. In terms of the political climate, the EU-Japan Economic Partnership Agreement (EPA) entered into effect, after a series of negotiations that began in April 2013, nearly a week after the mutual agreement, on 1 February 2019. One may be able to see the coincidence of trade agreement and adequacy decision. The European Commission repeatedly stated that the protection of personal data was ‘non-negotiable’ in the context of and trade agreement[33]. Reflecting this attitude, the data transfer agreement is separate from the trade agreement at least in text, both of which have become practically entangled in the name of ‘digital trade’[34]. The EPA includes a disclaimer which provides that each party may ‘define or regulate its own levels of protection in pursuit of or furthermore of its public policy objectives in areas’ of ‘personal data’ (Art.18.1(2)(h) in Chapter 18 Good regulatory practices and regulatory cooperation)[35]. Through ‘the world’s largest area of safe data flows’[36] between the EU and Japan, a practical observation should be undertaken to determine how this EPA provision will influence the mutual adequacy decision.

Japan’s adequacy decision was issued after receiving both the EDPB’s opinion[37] and an European Parliament (EP)’s resolution[38], both of which included several critical assessments, clarifications, and concerns regarding the Commission’s draft adequacy decision. Three important issues should be noted here before examining the substances of this decision and later developments in the next section. First, Japan’s adequacy decision was not comprehensive one, rather it was a partial decision that only applied to the commercial private sector. On the other hand, the Japanese public sector institutions are required to seek other options or accept a binding agreement in regard to data transfers from the EU. For instance, the National Police Agency of Japan and Europol reached an agreement on information sharing including transferring personal data[39] and the Science Council of Japan considered the impact of the partial adequacy decision for the public research institutions[40]. Similar to Canada’s private sector adequacy decision[41], the transfer and use of Passenger Name Records (PNRs) will prompt the EU to make a cautious agreement with Japan based on the lack of independent oversight and the absence of effective remedy for EU citizens, and a risk of processing indirectly sensitive data[42]. Second, the APPI alone is not adequate, and both the Supplementary Rules and official assurances of the Ministries regarding government access are essential requirements for Japan’s adequacy decision. It is questionable that both the Supplementary Rules and official assurances are binding and enforceable by the Japanese courts. Third and most importantly, while the adequacy decision is guaranteed for four years under the GDPR, Japan’s adequacy is subject to a first review within two years. The Commission will decide whether the two-year-cycle should be maintained (Decision (181)). This shorter review cycle will create a more intensive dialogue between the EU and Japan.

III- ANALYSING THE EDPB OPINION AND EP RESOLUTION

A- CONTENT PRINCIPLES

a) Concepts


40 Science Council of Japan held a symposium on the GDPR and the academic institutions in March 2019.

41 See Opinion 1/15, Avis rendu en vertu de l'article 218, paragraphe 11, TFUE, ECLI:EU:C:2017:592. The Court noted a clear and precise manner of transfer, the models and criteria of automated processing, prior review by a court or by an independent administrative body, limited retention period, conditional disclosure to the third country, a right to individual notification, and the oversight are required for the PNR agreement.

42 European Commission, Recommendation for a council decision to authorise the opening of negotiations for an Agreement between the European Union and Japan for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime, 27 September 2019. See also 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.

https://blogdroiteuropeen.com
As a starting point, the Constitution of Japan does not explicitly grant any rights to privacy nor right to protection of personal data, while the EU Charter of Fundamental Rights embraces both the right to respect private life and the right to protection of personal data. However, Japanese case law recognises the right to privacy both against public institutions and private relations. For instance, in the residential network (jukin-net) case, the Supreme Court of Japan held that since Article 13 of the Constitution provides that citizens’ liberty in private life shall be protected against exercise of public authority, and it can be construed that, as one of individuals’, every individual has the liberty of protecting his/her own personal information from being disclosed to a third party or being made public without good reason. In regard to private relations, the Civil Code 709 also applies to tort cases relating to privacy and personal data.

As for the scope of personal data, the most fundamental question raised by the EP is whether the APPI takes a harm-based approach in that cabinet order excludes harming an individual’s rights and interests considering their utilisation method (EP Resolution (13)). Contrary to the EU’s rights-based approach, Japanese law allows some exceptions such as the stipulation that personal data retained only for less than 6 months is outside the scope of access, rectification and utilisation suspension due to the low risk of harm to data subjects. Although this portion was modified by the Supplementary Rules (2) of the PPC, the rights-based versus harm-based approach was found in this aspect.

The differences between the APPI and the GDPR are also clear in that the APPI does not, in principle, regard IP addresses, device IDs or telephone numbers as personal information nor does it consider personal identification code since they are automatically assigned. By contrast, the CJEU and the European DPAs, in general, interpret them as personal data.

In addition to the definition of personal data, there is no clear distinction between ‘controller’ and ‘processor’ under the APPI, which also raises questions (EDPB (21)). The APPI provides for ‘trustee’ which is entrusted in handling personal data under the supervision by the original business operator.

In August 2019, a recruiting company with approximately annual 800,000 applicants created and sold the applicants scores regarding the possibility of declining the job offers. Without a clear explanation and consent from data subjects, this recruiting company specifically sold personal data to 35 contracting companies which gave personal data to the recruiting company as a ‘trustee’. In this regard, the role of ‘trustee’ primarily used to justify selling personal data. Based on a comparison with the GDPR, the APPI established more flexible divisions of responsibility between original business operators and ‘trustees’.

In this context, ‘joint controllership’ under the GDPR has some differences in ‘a jointly utilising person’ under the APPI. Joint controllership means that ‘two or more controllers jointly determine the purpose and means of processing’. While ‘a jointly utilising person’ under the APPI aims to clarify the prime power of handling complaints and access requests among the joint companies. In practice, a social plugin service may lead a divergent conclusion between a ‘joint controllership’ and ‘a jointly utilising person’, in which the former may share responsibilities among controllers in processing, but the latter may identify a single responsibility in complaint handling and access request.

b) Grounds for lawful and fair processing for
legitimate purposes

While the GDPR provides the rigid requirements for lawful processing, the APPI does not entail such obligations before processing. However, the APPI does prohibit the deceptive collection of personal data and information to the data subjects for handling personal data. Most notably, the APPI does not define consent nor does it outline any concept of withdrawal of consent (EDPB (89)). The PPC explains that implicit consent can be used on case-by-case judgement basis\(^1\). Indeed, pre-checked consent is sometimes used in Japanese business practices, which may not be compatible with the Planet 49 case in the EU\(^2\).

c) Purpose limitation principle

Although there is no concept of ‘compatibility’ in regard to purpose changes under the APPI, business operators can still change the purpose if it is ‘what can reasonably be considered as appropriately relevant for the original purpose’. The Supplementary Rules (3) provide that personal data transferred from the EU are also subject to the confirmation and record-keeping requirements under the APPI in order to specify the purpose of handling personal data.

d) Data quality and proportionality principle

Data quality is provided under the APPI as a matter of striving for business operators.

e) Data retention principle

As a matter of striving for business operators, the APPI provides for the deletion of personal data without delay when such utilisation has become unnecessary. Furthermore, some business industry has its own retention periods (eg. credit history is retained for up to five years in Credit Information Center\(^3\)).

f) Security and confidentiality principle

Details of security measures are provided in both the PPC Guidelines addition to the APPI. Unlike the GDPR’s 72-hour rule, however, there is no mandatory breach notification under the APPI. On the other hand, the PPC may be voluntarily notified (eg. 1,216 notifications in FY2018\(^2\)).

g) Transparency principle, the right of access, rectification, erasure and objection

Regarding the transparency principle, data subjects ‘can know’ the name of the business operators, purpose, and the procedures access, rectification and suspension of utilisation or deletion including a fee etc. Here, the languages of ‘can know’ mean that if data subjects wish to know, they can easily gain such information in terms of time and means (eg. visiting the business operator’s homepage)\(^2\). In a 2019 transparency enforcement case, the PPC issued an instruction against JapanTaxi for not providing intelligible explanations, regardless of the information presented on their homepage in regard to capturing the faces of taxi users inside tablets for advertisement purposes\(^4\).

Although this is not unique to the Japanese context, it is important to ensure that EU citizens have access to the purpose of utilisation once their data are transferred to Japan. However, linguistic barriers create a situation in which not all the Japanese business operators provide explanations in English or other EU languages in their privacy policies\(^5\).

The most important analysis of the rights under the APPI is that, unlike in the GDPR Art.23, retained personal data excludes in advance certain categories of data relating to national security or crime prevention by cabinet order instead of balancing between the rights and public interests in front (EDPB (95)). The same is true of the APPIHAO and the APPI-IAA by excluding the data relating to national security or crime prevention among public sector organisations. A closer examination of the extent of the limitation issue makes it doubtful that the exclusion from access, rectification, or the suspension of utilisation rights in advance is compatible with the essence of fundamental rights\(^6\). Furthermore, there

49 PPC, Q&A regarding the Guidelines on the Protection of Personal Information & Response in the case of Breach of Personal Data etc, FQA1-57 (12 November 2019).
50 Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49, ECLI:EU:C:2019:801 para 49. [...] any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including ‘by ticking a box when visiting an internet website’
51 https://www.cic.co.jp/confidence/possession.html#sst02 (in Japanese)
55 Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 11 April 2018, p.10 (A translation in one or more other languages should be provided where the controller targets data subjects speaking those languages).
is no clear balancing model under the APPI. In this regard, the EDPB noted the relevant documents were absent in order to demonstrate the restrictions to the individuals rights were ‘necessary and proportionate in a democratic society and respect the essence of fundamental rights’ (EDPB (22)). However, the judicial balancing test is referred in practices of data protection in Japan (Decision (8)). Again, one should realise that the APPI certainly uses ‘rights and interest’ in Art.1, the language of which still needs clarification in regard to its approach without any indications of ‘fundamental rights’ in the PPC guidelines and the relevant documents so far.

Some other differences should also be noted here. For one thing, business operators are granted a fee for access, rectification and suspension of utilisation or deletion. Furthermore, the right to deletion is not an independent right and business operators can either choose to suspend the utilisation of ‘or’ delete personal data with narrower requirements.67

h) Restrictions on onward transfers

One of the most complex parts of an adequacy decision is the restrictions on onward transfer, which may potentially impact other third countries. In the Japanese decision, the European Commission importantly wrote that ‘the requirements set forth in Supplementary Rule (4) exclude the use of transfer instruments that do not create a binding relationship between the Japanese data exporter and the third country’s data importer of the data and that do not guarantee the required level of protection. This will be the case, for instance, of the APEC Cross Border Privacy Rules (CBPR) System, of which Japan is a participating economy’ (Decision (79). See also EDPB (110-112)).

These sentences indicate that Japan can no longer rely on the APEC CBPR system for onward transfer. In its exclusion of the APEC channel for onward transfer, the Supplementary Rules (4) makes it seem as if the PPC is taking back its words in the Guidelines stipulating that the Japanese business operators can use the APEC CBPRs system for data transfers regardless of which third countries are listed on the PPC’s white list.58 Japan adequacy provides global insight into the complex relationship between the EU adequacy and APEC CBPRs.

i) Special categories of data

According to the Supplementary Rules (1), the special-care required personal information now covers the special categories of data listed in the GDPR. The equality question remains that personal data such as sexual orientation or labour union membership is protected as special-care required personal information with consent in collection only when it is transferred from the EU, while the domestic Japanese data are not treated as such.

j) Direct marketing

There is no specific provision regarding direct marketing regulation under the APPI (EDPB (115) & EP (18)), while other legislations (eg. the Act on Specified Commercial Transactions) does cover direct marketing.

k) Automated decision making and profiling

There is no regulation regarding automated decision making and profiling under the APPI (EDPB (121)). Profiling was tabled in the amendments of the APPI in 2015, which became a continuous topic for the future. However, as stated above, the recruiting case in Japan shows how the company uses artificial intelligence in the context of human resources to single out the possibility of accepting and declining job offers or identifying a given applicant’s level of qualification.

As the European Parliament concretely points out regarding the Japanese implications for Facebook/Cambridge Analytica case (EP (17)), the PPC issued instructions due to the possibility of affecting 100,948 individuals by way of the 104 users who installed the application (i.e., thisisyourdigitallife) in question. These instructions require the Facebook to provide intelligible explanations to users, obtain consent from data subjects and respond to deletion requests from data subjects. However, there was no mention of profiling in this case. Compared with the investigation report issued by the UK Information Commissioner’s Office, which asserts that profiling of individuals is used to target messages/political adverts at potential voters.

57 The Supreme Court of Japan on 31 January 2017 dismissed the right to be forgotten case where a man asked Google to delete his previous news relating to the child prostitution with a fine nearly 5 years ago. Decision of the Supreme Court, 31 January 2017, Minshu No.71 vol.1 p.63. Available at https://www.courts.go.jp/app/hanrei_en/detail?d=1511
61 See ICO, Investigation into the use of data analytics in political campaigns, 6 November 2018.
the PPC’s instructions address transparency instead of profiling itself.

**B- PROCEDURAL AND ENFORCEMENT MECHANISM**

**a) Competent independent supervisory authority**

The PPC was established in January 2016 through amendments to the APPI in 2015. The PPC has the highest level of independence within the administrative organisation law in Japan (apart from the Board of Audit of Japan under the Constitution Art.90). One chairperson and eight Commissioners are supported by the secretary through staffs, most of whom are posted from other Ministries.\(^{62}\)

**b) The data protection system which ensures a good level of compliance**

One of the most difficult part of the adequacy assessment process involves compliance due to the different business cultures between Japan and Europe. Prior to the APPI amendments in 2015, Professor Greenleaf analysed that ‘[t]he Japanese system does not provide evidence of its effectiveness’ \(^{63}\) and, after the APPI amendments in 2015, that the PPC does ‘not give any examples of specific penalties issued or compensation granted, either administrative or judicial’.\(^{64}\) These evaluations can be endorsed by the fact that neither the former competent Minister nor the new PPC had ever issued any fines under the APPI (EDPB (131) & EP (21)).

However, not everything can be explained based on the number of fines. For one reason, the number of violations is not always identical to the number of fines. Furthermore, some violations can be suspended or improved by persuasion or appeal other than fines. Although there is no objective quantification tool for assessing data protection compliance, one may realise that the Japanese business culture obliges the business operators to notify even minor data breach cases to PPC under the voluntary framework. In FY 2018, the PPC accepted 1,216 notifications of data breaches, of these 81.9 percent cases were minor one such as wrong delivery of documents or emails or loss of documents or electric devices.\(^{65}\)

With public apologies being issued even for minor data breaches, it is not wrong to state that the reputational risks of data breach trigger a precautious measure with enhanced compliance to Japanese data protection laws. The lack of enforcement with hard power by the PPC may reveal the weakness of these laws, while it is also true that such enforcement is not always necessary for accomplishing data protection in the context of the Japanese business culture.

**c) Accountability (Decision (73))**

While those are voluntary schemes, on 10 August 2017 the PPC had listed 44 authorised organisations, with the largest one, Japan Information Processing and Development Center (JIPDEC), alone counting 15,436 participating business operators (Decision (73)).

**d) The data protection system providing support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms**

While the PPC provides support to data subjects via telephone, there is no direct and binding remedy system under the APPI. As such, data subjects must seek litigations through the courts without any data protection NGOs in Japan. It is also true that the EU individuals may have difficulties accessing administrative and judicial redress (EDPB (134)). After the adequacy decision, the PPC prepared to take telephone calls from the EU in English or Japanese, but only in which data subjects were submitting complaints to the Japanese administrative authority (that is, not for complaints to business operators). \(^{66}\)

**C- GOVERNMENT ACCESS TO PRIVATE DATA FOR LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES**

While there are very limited even in Japanese languages, the most important sources in the adequacy decision involves government access. In this sense, Annex II provides a precious explanation of the Japanese legal system with strong assurances and commitments from the relevant Minister and high officials. Still, one may face the difficulty in assessing the government access to private data in Japan in the absence of sufficient

\(^{62}\) Although the adequacy decision does not require ‘complete’ independence, one may be able to remind the requirement for ‘complete’ independence in its staffs and equipment. See Case C-614/10, European Commission v Austria, ECLI:EU:C:2012:631 para 58. (…the attribution of the necessary equipment and staff to such authorities must not prevent them from acting ‘with complete independence’)


\(^{66}\) Complaint Mediation Line for Japanese administrative authorities’ handling of personal data transferred from the EU and the UK based on an adequacy decision, etc. Available at [https://blogdroiteuropeen.com/en/contactus/complaintmediationonline/](https://blogdroiteuropeen.com/en/contactus/complaintmediationonline/)
EU-JAPAN MUTUAL ADEQUACY DECISION

The EDPB is not in a position to assess whether these limitations to the rights of data subjects are limited to what would be considered strictly necessary and proportionate under EU law, and would thus be essentially equivalent to the rights provide to the EU data subjects.

Shortly before the adequacy decision in January 2019, the several newspaper articles published the facts that the Prosecutor’s Office was in possession of a list containing approximately 290 companies that give customers’ data to the Office on a voluntary basis. Furthermore, Culture Convenience Club Co., which is the largest royalty card company with over 70 million customers (more than half of the Japanese population), publicly announced that they had disclosed personal data to law enforcement agencies on a voluntary basis in order to contribute to the society. In the wake of this newspaper article, the National Police Agency responded in the Diet that the prefectural police do not have a coercive power to investigate the businesses through written inquiries on investigative matters even under the Code of Criminal Procedure, in which case they obtain a warrant from a court.

While there is a practical demand for criminal investigation by enquiry sheet, there are at least three remaining questions regarding government access to private data in Japan. First, the problem of ‘voluntary basis’ disclosure is not lawfulness of its system rather its ‘blackboxing’ of facts to the data subjects with a lack of transparency reports in Japanese businesses. As the EDPB pointed out, ‘figures on the number and types of requests, as well as on the answers provided by the controllers requested’ are almost all in the blackbox. On this issue, the adequacy decision cites the transparency report for a social media company LINE

Second, with a few exceptional cases granted by courts, there is no evidence that the Japanese law enforcement agencies abuse their power in order to carry out a massive surveillance of ordinary citizens. However, the question of government access does not concern the lack of evidence for power abuses. Rather, even if there is no such evidence, the overall architecture requires sufficient supervision and oversight to provide adequate and effective guarantees against abuse. Several types of supervisions are described in the Annex II, but the EU standard may pose questions about organisational supervision (EDPB (166), (173) & (184)). In addition, data subjects cannot truly seek a remedy without being exposed to the facts contained in personal data that are shared to law enforcement agencies on a voluntary basis.

Third, there is a technical question over whether a warrant issued by a court can solve all the government access cases in relation to protection of personal data, after the GPS tracking judgment by the Supreme Court.

In the case of GPS tracking with 19 cars attached in the theft case without a warrant, the Supreme Court of Japan held that ‘GPS tracking investigation necessarily entails monitoring of an individual’s behavior both continuously and comprehensively and can invade the individual’s privacy’ by entering into the private sphere under Constitution Art. 35 (Decision (114)). The Court further commented on the need for legislation for GPS tracking investigations instead of issuing inspection permits through warrants via case-by-case reviews (in Japan, 98.5 percent of warrant requests were granted in 2018). This judgement can be understood as the indicating the need for clear legal grounds in cases of

67 ‘[T]he EDPB is not in a position to assess whether these limitations to the rights of data subjects are limited to what would be considered strictly necessary and proportionate under EU law, and would thus be essentially equivalent to the rights provide to the EU data subjects.

68 ‘It is beyond the task of the EDPB to make a general assessment of the possible surveillance capabilities of the Japanese government.’

69 ‘[I]nits the Commission to assess whether this [voluntary basis disclosure] is compliant with the standard of being ‘essentially equivalent’ to the GDPR’

70 See e.g. Prosecutor listed how to obtain customers’ data and holds it from 290 companies, Tokyo newspaper, 3 January 2019 (in Japanese); Questioning information voluntary provision to police, Mainichi newspaper 22 January 2019 (in Japanese) Available at https://mainichi.jp/articles/20190121/k00/00m/040/224000c.


72 House of Representatives, Committee on Judicial Affairs, 198th Diet, National Police Agency, Commissioner-General’s Secretariat Counselor’s Statement, 15 May 2019. See Code of Criminal Procedure Art. 197 (2) (Public offices or public or private organizations may be asked to make a report on necessary matters relating to the investigation).

73 See ECtHR, Big Brother Watch and Others v The United Kingdom, 13 September 2018 Applications nos. 58170/13, 62322/14 and 24960/15 para 383 (referral to the Grand Chamber) [The Court affirmed the necessity of ‘the supervision and oversight of the bulk interceptions capable of providing adequate and effective guarantees against abuse’]

74 Judgement of the Supreme Court, 15 March 2017, Keishu vol.71 no.3 p. 13. https://www.courts.go.jp/app/hanrei_en/detail?id=3518 75 Article 35 of the Constitution provides that [(t)he right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause...].

76 Courts in Japan, The numbers of requesting and issuing warrants. https://www.courts.go.jp/vc-files/courts/2020/01_taiho.pdf (in Japanese). It is important to understand that this number should not be treated as a guesswork; one may recognise that judges pass almost all warrant requests by law enforcement agencies. Others may understand that the police are well prepared to request warrants only in necessary cases.
government access when investigations fall into the category of compulsory investigation with monitoring of an individual’s behavior both continuously and comprehensively.

IV- AMENDMENTS TO FUTURE ADEQUACY REVIEWS

A- PREPARING FOR THE FIRST ADEQUACY REVIEW

The adequacy decision process motivated the Japanese stakeholders to realise how the APPI and the relevant laws should be improved before the first adequacy review, which is scheduled for January 2021. As the most important development after the adequacy decision, the Japanese cabinet decided to submit the amendments bill to the APPI in the Diet on 10 March 2020[77]. Here is an overview of the amendments bill[78].

First, the amendments bill enhances the individual right to suspend utilisation in cases of involving the potential violations of data subject’s rights and legitimate interests. As such, short retention (ie, less than six months) personal data also falls into the scope of retained personal data for access, rectification, and the suspension of utilisation in order to reflect the Supplementary Rules (2).

Second, the duties of business operators are added to the bill; data breach notifications thus become mandatory in cases of potential significance regarding the rights and interests of an affected individual. The bill also prohibits use of personal information in ways that may potentially facilitate or induce illegal or unjustifiable conducts.

Third, and probably the most controversial topic in the bill, is the concept of personally relevant information, which is defined as a personal data for the recipient, but is not necessarily as such for the sender. This concept supposes that the abovementioned recruiting company case where the company intentionally avoided the APPI obligation by hashing personal data but were knowingly identified by the recipient. Such a bypass can be used through Data Management Platform, which is the target of this new concept of personally relevant information. In addition, pseudonymisation was introduced through the bill so that the businesses could promote utilisation. In 2015 amendments, anonymously processed information was introduced not many companies have used such anonymously processed information due to the risk of re-identification and complexity of anonymous processing[79]. Thus, the bill again adds a new data category of pseudonymisation, in which data utilisation entails relaxed obligation for access requests.

Fourth, the amount of fines are increased to a maximum 100 million yen for the legal person (the current APPI lists a maximum of a half million yen).

Fifth, the PPC expands the authorisation scheme for the organisations to ensure the proper handling of personal information in regard to their respective business types.

Finally, foreign business operators are subject to the collection of reports and orders backed by penalty. The intention of this newly outlined PPC power against foreign business operators can be understood as a ‘GAFA (Google-Amazon-Facebook-Apple)’ measure, which coincides with the Bill on the Act on Improvement of Transparency and Fairness in Trading on Specified Digital Platforms[80].

The partial adequacy decision may also be improved in the future through this amendments bill. The Cabinet Secretariat established the Taskforce on the Review of System of Protection of Personal Data in December 2019 in order to integrate divisive systems in the private and public sectors with a view to submitting another amendments bill in 2021. These ambitious developments of reviews in the protection of personal data were quite possibly motivated by the adequacy talks with the EU and the prospect of future adequacy reviews.

B- ADEQUACY AS A TOOL FOR CONVERGENCE RATHER THAN DATA TRANSFER

On the same day of the mutual adequacy decision, Prime Minister of Japan Abe declared ‘data free flow with trust’ at the World Economic Forum[81]. Such an initiative was shared by the European Commission[82].

79 According to the newspaper research on the in-house or corporate lawyers, only 14 percent of the companies use anonymously processed information. See Anonymous processed information, Nikkei newspaper, 27 January 2020 p. 11.

https://blogdroiteuropeen.com
this sense, the adequacy decision may well be explained through a political premise. The political nature of EU adequacy and its legal effects may motivate ‘the political will’ of a third country to reconsider the domestic data protection system. This is indeed the case for Japan.

The EU-Japan mutual adequacy decisions may be a successful political agreement, but one should note the extent to which it unites two systems with different philosophical ideas on data protection. For instance, the Japanese initiative of ‘data free flow with trust’ is embedded in the WTO reform proposal. It is true that personal data can be discussed in the economic dimension, however, the EU’s rationale for the adequacy decision stemmed from a human rights philosophy, which may be alien to the WTO solution. In this regard, it is too early to evaluate how the EU-Japan mutual adequacy decision will progress the convergence of data protection, whether it is taken as a human rights philosophy or an act of commercial reciprocity.

By nature, adequacy has by nature a narrower meaning in the sense that the EU authorises data transfers to the third country. In reality, the adequacy has bigger impacts in that the third country is expected to meet the ‘essentially equivalent’ standard to thouse outlined in the GDPR as an ‘instrument of harmonisation’. In fact, the GDPR has double methods of exporting its essence of a fundamental right by adequacy and extraterritorial effect. By adequacy, the EU maintains the essential equivalence to the third countries. By extraterritorial effect, the EU extends its essence of data protection to the third countries. As these two tools are designed to maintain its core value of fundamental rights, the EU strategy for protection of personal data now becomes a firm basis for exporting its philosophy to third countries including Japan. However, adequacy is not the European imperialism in the digital world, rather it is a pragmatic, and quite possibly politically motivated opportunity to establish trust through convergence the different systems of protecting personal data. What is considered sensitive in the EU may not always be sensitive in Japan and vice versa. However, both the EU and Japan streamline the legal frameworks in the face of similar risks posed to personal data protection. For instance, the recent ‘Communication on Building Trust in Human Centric Artificial Intelligence’ places people at the centre of the development of AI. In Japan, the Cabinet Office publicised the ‘Social Principles of Human-centric AI’ which mentions use of AI as the human’s instruments. These two policy papers coincide in their human centric approaches in an age AI, which may create new opportunities to converge the essence of fundamental rights.

In the Japanese Edo-era for over two centuries (1639-1854), the Japanese islands were closed and isolated from foreign policies, which are called ‘sakoku’ in Japanese. In this regard, the initial Japanese data protection laws and policies may be illustrated as ‘sakoku’. Indeed, Japan did not belong to a member of international privacy community, nor did it have an independent supervisory authority. Later on, in 1991, both the European Community and Japan agreed to strengthen their co-operation based on ideals of freedom, democracy, the rule of law, human rights, and market economy. One may be able to describe that the EU-Japan mutual adequacy decision can serve as a digital ‘kaikoku (opening the country)’ for data free flow with trust. In sum, the mutual adequacy decision is a forward-looking political choice that provides mutual benefits while shaping the ‘essence’ of a data protection philosophy for Japan.

83 See Elaine Fahey & Isabella Mancini, The EU as an intentional or accidental convergence actor? Learning from the EU-Japan data adequacy negotiations, International Trade Law and Regulation (2020).
89 European Commission, Building Trust in Human-Centric Artificial Intelligence, 8 April 2019. See also European Commission, White Paper on Artificial Intelligence- A European approach to Excellence and Trust, 19 February 2020.
92 Joint Declaration on Relations between the European Community and its Member States and Japan, 18 July 1991.