Council of the
European Union

Brussels, 18 December 2018
(OR. en)

15699/18

DATAPROTECT 275
JAI 1322
DAPIX 389
FREMP 244
DIGIT 259
RELEX 1116
WTO 344
SERVICES 75
MI 1015

COVER NOTE

From:	European Data Protection Board
To:	Delegations
Subject:	Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan adopted on 5 December 2018

Delegations will find in Annex the Opinion of the European Data Protection Board (EDPB) on the draft implementing decision of the European Commission on the adequate protection of personal data by Japan pursuant to the General Data Protection Regulation (GDPR).

Opinion 28/2018

regarding the European Commission Draft Implementing Decision

on the adequate protection of personal data in Japan

Adopted on 5 December 2018

Table of contents

1 EXECUTIVE SUMMARY 4

1.1 Areas of convergence 5

1.2 General challenges 5

1.3 Specific commercial aspects 6

1.3.1 Concerns of the EDPB with regards to key data protection principles 6

1.3.2 Need for clarification 7

1.4 On the access by public authorities to data transferred to Japan 7

1.5 Conclusion 7

2 INTRODUCTION 8

2.1 Japan's data protection framework 8

2.2 Scope of the EDPB's assessment 9

2.3 General comments and concerns 10

2.3.1 Specificities of this type of adequacy decision 10

2.3.2 Certainty of translations 10

2.3.3 Sectorial Adequacy 11

2.3.4 Binding nature of Supplementary Rules and of PPC Guidelines 11

2.3.5 Periodic review of the adequacy finding 12

2.3.6 International commitments entered into by Japan 12

2.3.7 Powers of DPAs to bring actions concerning the validity of an adequacy decision before a court 13

3 COMMERCIAL ASPECTS 13

3.1 Content principles 13

3.1.1 Concepts 13

3.1.2 Grounds for lawful and fair processing for legitimate purposes 16

3.1.3 The transparency principle 17

3.1.4 Restrictions on onward transfers 18

3.1.5 Direct marketing 21

3.1.6 Automated decision making and profiling 21

3.2 Procedural and enforcement mechanisms 22

3.2.1 Competent independent Supervisory Authority 22

3.2.2 The data protection system must ensure a good level of compliance 22

3.2.3 The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms 23

4 ON THE ACCESS BY PUBLIC AUTHORITIES TO THE DATA TRANSFERRED TO JAPAN 24

4.1 Law enforcement access to data 25
4.1.1 Procedures for accessing data in the field of criminal law 25
4.1.2 Oversight in the field of criminal law 27
4.1.3 Redress in the field of criminal law 30
4.2 Access for national security purposes 36
4.2.1 Scope of surveillance 36
4.2.2 Voluntary disclosure in case of national security 38
4.2.3 Oversight 38
4.2.4 Redress mechanism 40

The European Data Protection Board

Having regard to Article 70.1(s) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING OPINION:

1 EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision on the adequate protection of personal data by Japan pursuant to the General Data Protection Regulation (hereinafter: GDPR)[1] on 5 September 2018[2]. Following this, the European Commission initiated the procedure for its formal adoption.

2. On 25 September 2018, the European Commission asked for the opinion of the European Data Protection Board ("EDPB")[3]. The Commission was requested to provide the EDPB with all the necessary documentation with regards to this country, including any relevant correspondence with the government of Japan.

3. In the light of the discussions held with the EDPB, the European Commission modified twice its draft adequacy decision, and sent its last version on 13 November 2018[4] The EDPB has based its present Opinion on this latest version of the draft implementing decision (hereinafter "draft adequacy decision").

4. The EDPB's assessment of the level of protection ensured by the Commission's adequacy decision has been made on the examination of the decision itself as well as on the basis of an analysis of the documentation made available [5]– by the Commission[6].

5. The EDPB focused on the assessment of both the commercial aspects of the draft adequacy decision and on the government access to personal data transferred from the EU for the purposes of law enforcement and national security, including the legal remedies available to EU individuals. The EDPB

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] See Press release http://europa.eu/rapid/press-release_IP-18-5433_en.htm.
[3] Pursuant to Article 70 (1) (s) of the GDPR.
[4] See Annex I of the EDPB Opinion for the updated version of the draft European Commission implementing decision.
[5] The EDPB based its analysis on translations provided by the Japanese authorities verified by the European Commission
[6] See Annex II of the EDPB Opinion for the list of documents not provided by the European Commission to the EDPB.

also assessed whether the safeguards provided under the Japanese legal framework are in place and effective.

6. The EDPB has used as a main reference for this work its adequacy referential[7] adopted in February 2018.

1.1 Areas of convergence

7. The EDPB's key objective has been to give an opinion to the European Commission on the level of protection afforded to individuals in the Japanese framework. It is important to recognise that the EDPB does not expect the Japanese legal framework to replicate European data protection law.

8. However, the EDPB recalls that to be considered providing an adequate level of protection, the case law of the CJEU as well as Article 45 of the GDPR require that the third country's legislation needs to be aligned to the essence of the fundamental principles enshrined in the GDPR. In the areas of data protection, the EDPB further notes that there are key areas of alignment between the GDPR framework and the Japanese framework on certain core provisions such as data accuracy and minimisation, storage limitation, data security, purpose limitation and an independent supervisory authority, the Personal Information Protection Commission (PPC).

9. In addition to the above, the EDPB welcomes the efforts made by the European Commission and the Japanese authorities to ensure that Japan provides an adequate level of protection to that of the GDPR especially by filling the gaps between the GDPR and the Japanese data protection framework through the adoption of additional rules by the PPC applicable only to personal data transferred from the EU to Japan, the Supplementary Rules. For example, the EDPB notes that the PPC agreed to treat further categories of data as sensitive data (sensitive data under the Japanese legislation do not include sex orientation nor trade union membership). In addition, the Supplementary Rules ensure that data subject rights will apply to all personal data transferred from the EU, irrespective of their retention period (whereas the Japanese legal system provides that data subject rights do not apply to personal data that are set to be deleted within a period of six months).

10. The EDPB also notes the efforts of the European Commission in strengthening the adequacy decision in response to the concerns raised by the EDPB.

1.2 General challenges

11. Nonetheless, challenges remain and the EDPB suggests the following as the main areas that should be strengthened and closely monitored in the Japanese system.

12. The first challenge relates to the monitoring of this new architecture of adequacy, which is combining an existing legal framework with specific Supplementary Rules, to ensure that it will be a sustainable and reliable system that will not raise **practical issues regarding the concrete and efficient compliance** by Japanese entities and enforcement by the PPC.

13. Secondly, the EDPB takes note of the repeated commitments and reassurances of the European Commission and of the Japanese authorities regarding the binding and enforceable nature of the Supplementary Rules whilst inviting the European Commission to **continuously monitor their binding nature and effective application in Japan** as their legal value is an absolutely essential element of the EU – Japan adequacy. With respect to the PPC guidelines, the EDPB would welcome clarifications in

[7] WP254, Adequacy Referential, 6 February 2018.

the draft adequacy decision in relation to **their binding nature and asks the Commission to attentively monitor this aspect**[8].

1.3 Specific commercial aspects

14. In the area of the commercial aspects of the draft EU – Japan adequacy decision, the EDPB has some specific concerns and would like to request clarifications on some important matters.

1.3.1 Concerns of the EDPB with regards to key data protection principles

15. The EDPB welcomes that the Supplementary Rules exclude that personal data transferred from the EU is further transferred to a third country on the basis of APEC – CBPRs. In addition, the EDPB recognises that in its new draft of the adequacy decision, the European Commission committed itself to suspend the adequacy decision when onward transfers no longer ensure the continuity of protection.

16. Under the Japanese legislation, one of the legal basis for onward transfers is the recognition of a third country as providing an adequate level of protection to that of Japan. However, the assessment of a third country as adequate by Japan seems not to include the specific "Supplementary Rules" negotiated between the European Commission and the PPC which are only applicable to EU personal data in order to provide for a level of protection essentially equivalent to the GDPR standards. It follows that EU personal data that are transferred from Japan to another third country not recognised as having an essentially equivalent data protection framework to the GDPR on the basis of a Japanese adequacy will not necessarily enjoy the specific protection for EU personal data anymore.

17. **It should however be borne in mind that onward transfers of personal data may occur to third countries which become subject to a possible later Japanese adequacy decision. These third countries may not have been subject of a previous assessment or adequacy finding of the EU. At this point the COM should take over its monitoring role and ensure the level of protection of EU data is maintained or consider suspension of this adequacy decision.**

18. Moreover, the EDPB has concerns in relation to the **consent and transparency obligations** of data controllers (PIHBOs). The EDPB made a careful check of these elements for the reason that, differently to European data protection law, the use of consent as a basis for processing and for transfers has a central role in the Japanese legal system. For example, the EDPB has concerns regarding the notion of consent which is not defined in a way to include the right to withdrawal, an essential element under EU law to ensure the data subject's genuine control over his/her personal data. Regarding the transparency obligations of a PIHBO, there are doubts as to whether proactive information is given to data subjects.

19. The EDPB is concerned that the **Japanese redress system** may not be of easy access to individuals in the EU needing support or wishing to make a complaint in light of the fact that PPC's support is available via Helpline and in Japanese only. The same issue exists with the mediation service provided by the PPC as the system is not publicised on the English version of the PPC's website whilst important informative documents, such as the frequently asked questions on the APPI, are also available in Japanese only. In this respect, the EDPB would welcome if the Commission could discuss with the PPC the possibility of setting up an online service, at least in English, aimed at providing support to, and handle complaints of, individuals in the EU – similar to the one envisaged in Annex II of this adequacy decision. The European Commission will also need to monitor closely the effectiveness of sanctions and of relevant remedies.

[8] See Section 1.3.4 of the present opinion for more information.

1.3.2 Need for clarification

20. The EDPB would welcome assurances on some aspects of the draft adequacy decision on which further clarification is still needed.

21. These relate for example, to some key concepts of the Japanese legislation. More specifically, there is a lack of clarity around the **status of the so-called "trustee"** - a term which resembles to the one of the data processor under the GDPR but whose ability to determine and change the purposes and means of processing of personal data remains ambiguous.

22. The EDPB would also need assurances due to lack of the relevant documents, on whether the **restrictions to the rights of individuals** (in particular, rights of access, rectification, and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights.

23. The EDPB would also expect that the European Commission closely monitors the effective protection of **personal data transferred from the EU to Japan, based on the draft adequacy decision, throughout their whole "life cycle"** even though the Japanese legislation imposes a record keeping obligation of the origin of the data for a maximum of three years.

1.4 On the access by public authorities to data transferred to Japan

24. The EDPB has also analysed the legal framework for Japanese governmental entities when accessing personal data transferred from the EU to Japan for law enforcement or national security purposes. While acknowledging the reassurances provided by the Japanese government, referred to as the Annex II to the draft adequacy decision, the EDPB has identified a number of aspects for clarifications and of concern, of which the following should be highlighted.

25. In the area of law enforcement, the EDPB notes that the legal principles applying to access data often appear to be similar to the rules in the EU, to the extent they are available. The lack of available translations of several legal texts and of relevant case law make it difficult, however, to conclude that all the procedures for accessing data are necessary and proportionate and that the application of those principles are applied in a way which is "essentially equivalent" to EU law.

26. In the area of national security, the EDPB recognises that the Japanese government has restated that information may only be obtained from freely accessible sources or through voluntary disclosure by companies, and that it does not collect information on the general public. It is aware, however, of concerns expressed by experts and in the media, and would welcome further clarification on surveillance measures by Japanese governmental entities.

27. As to the legal redress of EU individuals, in the area of law enforcement as well as national security, the EDPB welcomes that the European Commission and the Japanese government have negotiated an additional mechanism for EU individuals to provide them with an additional redress avenue, and thereby extending the powers of the Japanese data protection authority. However, a point of concern remains that this new mechanism does not entirely compensate for the shortcomings of oversight and redress under Japanese law. The EDPB thus seeks for further clarifications in order to ensure that this new mechanism does fully compensate those shortcomings.

1.5 Conclusion

28. The EDPB considers that this adequacy decision is of paramount importance. As the first adequacy decision since the entering into force of GDPR, it will constitute **a precedent for future adequacy**

applications as well as **for the review of the adequacy decisions rendered under Directive 95/46[9].** It is also important to underline that individuals are more and more conscious of the impact of globalisation on their privacy and turn to their supervisory authorities to ensure that adequate guarantees are in place when their personal data are transferred abroad. In light of these implications, the EDPB believes that the European Commission should ensure that there are no shortcomings in the protection offered by the EU-Japan adequacy and that this specific type of adequacy is aligned with the requirements of Article 45 of the GDPR.

29. The EDPB welcomes the efforts made by the European Commission and the Japanese PPC to align as much as possible the Japanese legal framework to the European one. **The improvements** brought in by the Supplementary Rules to bridge some of the differences between the two frameworks are very important and well received.

30. However, following a careful analysis of the Commission's draft adequacy decision as well as of the Japanese data protection framework, the EDPB notices that **a number of concerns, coupled with the need for further clarifications, remain**. Further, this specific type of adequacy combining an existing national framework with additional specific rules also raises questions about its operational implementation. In light of the above, the EDPB recommends the European Commission to address the concerns and requests for clarification raised by the EDPB and provide further evidence and explanations regarding the issues being raised. The EDPB also invites the European Commission to conduct a review of this adequacy finding (at least) every two years and not every four years as suggested in the current draft adequacy decision.

2 INTRODUCTION

2.1 Japan's data protection framework

31. Japan's data protection framework was modernized very recently, in 2017. This framework comprises several pillars, at the centre of which there is a general statutory law, the Act on Protection of Personal Information (APPI). Another important piece of legislation is the Cabinet Order to Enforce the APPI ("Cabinet Order") which specifies certain core principles of the APPI.

32. Based on a Cabinet decision, adopted on 12 June 2018[10] and Article 6 of the APPI, the PPC was given the power to "*take necessary action to bridge the differences of the systems and operations between Japan and the concerned foreign country in view of ensuring appropriate handling of personal information received from each country*"[11]. The Cabinet decision also suggests that the rules adopted by the PPC supplementing or going beyond those laid down in the APPI would be binding and enforceable on the Japanese business operators[12].

33. Accordingly, the PPC engaged in negotiations with the European Commission and adopted, in June 2018, stricter rules to the ones of the APPI and the Cabinet Order to be applied to data transferred from the EU. These are the 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,

[9] Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[10] The EDPB notes that according to the draft adequacy decision this Cabinet Decision was adopted on 12 June 2018. However, the EDPB was only provided with the draft version of the Cabinet Decision, dated April 2018.
[11] Cabinet Decision of April 25th, 2018.
[12] See section 1.3.4 below for more information.

hereafter "Supplementary Rules"[13]. These Supplementary Rules are also annexed to the draft implementing Commission decision published in July 2018.

34. It is important to note that the Supplementary Rules are only applicable to personal data transferred from the European Union to Japan on the basis of the adequacy decision and aim at enhancing the applicable protection to those data. As such they do not apply to personal data of individuals in Japan or coming from other countries than the ones of the EEA.

35. Further, the EDPB would like to draw attention to the fact that the amended APPI came into force on May 30, 2017 and the PPC in its current form was established in 2016. Moreover, the Supplementary Rules negotiated by the PPC with the European Commission have yet to enter into force as that will depend on the recognition by the European Commission of Japan as a jurisdiction adequate to the one in the EU.

2.2 Scope of the EDPB's assessment

36. The European Commission's draft adequacy decision is the result of an assessment of the Japanese data protection rules, followed by negotiations with the Japanese authorities. The outcome of these negotiations is notably reflected in the two annexes attached to the draft adequacy decision: the first one provides for additional protections that Japanese business operators will have to apply to the processing of personal data transferred from the EU, while the second one contains assurances and commitments from the Japanese government concerning public authorities' access to data.

37. The EDPB examined the Japanese data protection framework, the Supplementary Rules negotiated by the European Commission and the assurances and commitments from the Japanese government. The EDPB is expected to provide an independent opinion on the European Commission's findings, identify insufficiencies in the adequacy framework, if any, and endeavour to propose alterations or amendments to address these.

38. As mentioned in the EDPB adequacy referential, *"the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country"*[14].

39. Nonetheless, the EDPB received most of the documents in English translations, referenced to in the draft adequacy decision, which form an essential part of the Japanese legal system. The EDPB, therefore, renders the present opinion on the basis of the analysis of available documents in English. The EDPB took into account the applicable data protection framework in the European Union, including Article 8 of the European Convention on Human Rights (hereinafter: ECHR) protecting the right to private and family life as well as Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter: the Charter) respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial. In addition to the above, the EDPB considered the requirements of GDPR as well as looking at the relevant jurisprudence.

40. The objective of this exercise is to ensure that the Japanese data protection framework is essentially equivalent to that of the European Union. The concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. It is important to recall the

[13] Supplementary Rules, Annex I of the Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, sent to the EDPB on September 2018.-
[14] WP254, p.3.

standard set by the CJEU in Schrems, namely that – while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU – "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]"[15]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective, if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules[16].

2.3 General comments and concerns

2.3.1 Specificities of this type of adequacy decision

41. The EU-Japan adequacy is the first one to be examined against the new legal backcloth of GDPR. This renders the work of the EDPB all the more important in light of the effects of this draft adequacy decision for future adequacy applications.

42. The EU – Japan adequacy would also be the first mutual one. When and if the EU recognises Japan as providing an essentially equivalent level of protection to the one of the GDPR, Japan will also issue its own adequacy decision under Article 24 of the APPI, recognising the EU as offering an adequate level of protection under the Japanese data protection framework. Thus this envisaged Japan – EU adequacy is of a particular nature which the EDPB has taken into account in its assessment. As mentioned above, the Japanese PPC has negotiated specific, stricter rules with the European Commission, applicable only to personal data transferred from the EU. These stricter rules are binding and enforceable according to the Cabinet Decision and are to be complied with by all Personal Information Handling Business Operators (hereafter PIHBOs) in Japan when processing personal data coming from the EU under this draft adequacy decision.

43. The European Commission has therefore based its adequacy finding not only on the existing general Japanese data protection framework but also on these specific rules. The fact that Supplementary Rules were required to complement the APPI is indicative of the fact that the European Commission acknowledges that the Japanese data protection legislation is not, per se, essentially equivalent to the GDPR.

44. **In light of the above-mentioned issues, the EDPB invites the European Commission to ensure that this new architecture of adequacy, the first to be adopted under the GDPR, relying on Supplementary Rules, will be a sustainable and reliable system that will not raise practical issues regarding the concrete and efficient compliance by Japanese entities and enforcement by the PPC.**

2.3.2 Certainty of translations

45. Like the European Commission, the EDPB has worked on the basis of English translations provided by the Japanese authorities[17]. The EDPB calls the European Commission to clarify that it has based its draft adequacy decision on the English translations received and verify the quality and certainty of these translations regularly.

---

[15] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74).
[16] WP254, p.2.
[17] The European Commission has verified these translations.

2.3.3 Sectorial Adequacy

46. The adequacy finding of this draft adequacy decision is limited to the protection of personal information by PIHBOs within the meaning of the APPI. This means that the adequacy is sectorial as it only applies to the private sector, excluding from its scope transfers of personal data between public authorities and bodies. Currently, the European Commission briefly mentions this specificity of the scope of the adequacy in recital 10 of the draft adequacy decision.

47. **The EDPB invites the European Commission to explicitly mention the sectorial nature of this adequacy finding in the title of the implementing decision as well as in its Article 1 in accordance with Article 45 (3) GDPR.**

2.3.4 Binding nature of Supplementary Rules and of PPC Guidelines

48. Article 6 of the APPI mentions that "the government shall...take necessary legislative and other action so as to be able to take discreet action for protecting personal information that especially requires ensuring the strict implementation of its proper handling in order to seek enhanced protection of an individual's rights and interests, and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework." Although the government is clearly identified in this Article of the APPI as competent to take such legal action, it does not refer directly to the PPC as the competent body to adopt specific rules[18]. Due to time constraints, the EDPB was unable to gather, review and examine existing evidence on this point.

49. **In light of the importance of this issue, the EDPB takes note of the repeated commitments and reassurances of the European Commission and of the Japanese authorities regarding the binding and enforceable nature of the Supplementary Rules. The EDPB invites the European Commission to continuously monitor their binding nature and effective application in Japan as their legal value is an essential element of the EU – Japan adequacy.**

50. Moreover, the European Commission makes reference in several sections of its draft adequacy decision to the PPC Guidelines (Guidelines).

51. Although the European Commission clarifies that the Guidelines provide an authoritative interpretation of the APPI in recital 16 of its draft adequacy decision, in the same recital it makes reference to the binding nature of these Guidelines: "According to the information received from the PPC, those Guidelines are considered as binding rules that form an integral part of the legal framework, to be read together with the text of the APPI, the Cabinet Order, the PPC Rules and a set of Q&A prepared by PPC."[19]

52. However, the understanding of the EDPB, based on the same information provided by the PPC, is that the Guidelines are not legally binding. Rather, they provide an 'authoritative interpretation' of the law. The PPC argues that the Guidelines are followed by PIHBOs in practice, used by the PPC for enforcing

[18] According to an article published in July 2018, when the Supplementary Rules were in a draft, the legal binding nature of these Rules was likely to be the object of internal debate in the country. See Fujiwara S., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (July 2018): p. 19.

[19] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, Recital 16.

the law against PIHBOs and used by courts when rendering their judgment. However, these elements do not constitute sufficient evidence that the Guidelines are legally binding norms.

53. **The EDPB would welcome clarifications in the adequacy decision in relation to the binding nature of the PPC Guidelines and asks the European Commission to attentively monitor this aspect.**

54. According to the PPC, the Guidelines are followed in practice nevertheless as it is local custom. The PPC mentions that the Japanese courts use the PPC Guidelines to render their judgments when applying APPI rules. The European Commission makes reference to a court ruling[20] dating from 2006 to provide evidence that the Japanese courts base themselves on guidelines for their findings. Despite the fact that the EDPB was not provided with this court ruling, the EDPB would appreciate if the European Commission could provide, if available, a more recent court ruling, either in the field of data protection or in another sector where the Japanese courts have used the PPC Guidelines or other similar guidelines as a basis of their decision.

2.3.5 Periodic review of the adequacy finding

55. Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. According to the EDPB adequacy referential[21], this is a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

56. Taking into account a number of factors, including the fact that the APPI entered into force in 2017, that the PPC was established in 2016 and that there is no information nor evidence on the practical application of the Supplementary Rules yet, **the EDPB invites the European Commission to conduct a review of this adequacy finding (at least) every two years and not every four years as suggested in the current draft adequacy decision.**

2.3.6 International commitments entered into by Japan

57. According to Article 45 (2) (c) of the GDPR and the adequacy referential[22], when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data ("Convention 108+"[23] and its Additional Protocol should be taken into account.

58. **In this regard, the EDPB notes that Japan is an observer of the Consultative Committee of Convention 108+.**

---

[20] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, page 5, footnote 16, "Osaka District Court, decision of 19 May 2006, Hanrei Jiho, Vol. 1948, p. 122.

[21] WP254, p.3.

[22] WP254, p.2.

[23] Convention for the protection of individuals with regard to the processing of personal data, Convention 108+, 18 May 2018.

2.3.7 Powers of DPAs[24] to bring actions concerning the validity of an adequacy decision before a court

59. The EDPB underlines that although recital 179 of the draft adequacy decision only mentions cases where a DPA has received a complaint questioning the compatibility of an adequacy decision with the fundamental rights of the individual to privacy and data protection, this statement is to be understood as an example of situations, where a DPA can bring the matter before a national court, which could also be possible in the absence of a complaint, rather than as a restriction to the powers provided to DPAs under the GDPR and national laws of the Member States in this regard. Indeed, the provisions of the GDPR include both the power to suspend data transfers even when based on an adequacy decision and to bring an action concerning the validity of an adequacy decision, are not limited to cases where they have received a complaint, should their national law grant them the power to do so more broadly and independently from a complaint, in accordance with the relevant provisions of the GDPR.

60. **The EDPB invites the European Commission to clarify in its draft adequacy decision that the power of supervisory authorities to bring an action against the validity of an adequacy decision following a complaint is just an illustration of the broader powers of DPAs following from the GDPR, which include the power to suspend transfers and to bring an action concerning the validity of an adequacy decision in the absence of a complaint should their national law provide it.**

3 COMMERCIAL ASPECTS

3.1 Content principles

61. Chapter 3 of the Adequacy Referential is dedicated to the "Content Principles". A third country's or international organisation's system must contain them in order to regard the level of protection provided as essentially equivalent to the one guaranteed by EU legislation. The EDPB acknowledges the fact that the Japanese legal system pursues a different approach to that of the GDPR in order to give effect to the right to privacy. Although the right to privacy is not enshrined in the Japanese Constitution per se, it has been recognised as a constitutional right via case law as also referenced in the European Commission's decision[25].

62. Especially due to the fact that the Japanese approach noticeably differs from the European one, it has to be observed carefully whether, not only single aspects, but the system as a whole ultimately provides an "essentially equivalent" level of protection. This means, that potential "shortcomings" concerning one content principle might be compensated by some other aspects providing adequate checks and balances.

3.1.1 Concepts

63. Based on the adequacy referential, basic data protection concepts and/or principles should exist in the third country's legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in the European data protection law. For example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data"[26].

---

[24] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.
[25] The EDPB has not been provided with the English translation of this Court decision. See Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, footnote 9
[26] WP254, p.4.

64. The APPI also includes a number of definitions such as, among others, those of "personal information", "personal data", "personal information handling business operator". **However, it seems that the APPI does not include a definition of the term "handling of personal data" which is similar to the term "processing of personal data".**

65. Regarding the definition of the term "handling of personal data", the PPC provided written answers to the EDPB's question on this definition. The European Commission quoted this answer to the draft Commission decision *"While the APPI does not use the term "processing", it relies on the equivalent concept of "handling" which, according to the information received by the PPC, covers "any act on personal data" including the acquisition, input, accumulation, organisation, storage, editing/processing, renewal, output, reassure, output, utilization, or provision of personal information."*[27]

66. However, since the text of reference for this definition has not been provided, the EDPB invites **the European Commission to closely monitor that the definition of the abovementioned concept, as provided by the PPC, is effectively followed in practice.**

3.1.1.1 Concept of data processor and obligations of a "trustee"

67. As mentioned above, the adequacy referential requires that basic data protection concepts and/or principles should exist in the third country's legal framework.

68. The APPI includes a definition of a "personal information handling business operator" which according to the European Commission comprises both the terms of a data controller and a data processor as provided by the GDPR and does not distinguish between the two[28]. However, the APPI also includes a term "trustee" in its Article 22, which in some ways resembles the term of a data processor under the GDPR.

69. As explained by the PPC in its answers provided to the EDPB, and also included in the European Commission's draft adequacy decision, a trustee is considered as the equivalent of a data processor under the GDPR – entrusted with the handling of personal data by a PIHBO. This trustee has the same obligations and rights as any PIHBO, including the ones of the Supplementary Rules for personal data transferred from the EU. The PIHBO that entrusts the handling of personal data to a trustee is bound to "exercise necessary and appropriate supervision"[29] over the trustee.

70. **The EDPB invites the European Commission to explain the trustee's status and obligations when the trustee changes the purposes and means of processing and clarify whether the data subject's consent remains a necessary condition for such change of purpose or determination of means[30].**

---

[27] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, recital 17.

[28] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, recital 35.

[29] Article 22 of the Amended Act on the Protection of Personal Information (APPI), put into effect on May 30, 2017.

[30] Art. 23 para 5 (i) APPI. See also section on the transparency principle below.

3.1.1.2 Concept of retained personal data

71. The APPI contains the concept of "retained personal data" which is considered to be a sub-category of personal data. According to the APPI, the provisions relating to the data subject's rights[31] only apply to retained personal data. The definition of retained personal data is included in Article 2(7) of the APPI.

72. Retained personal data are the personal data other than those that (i) are set to be deleted within a period of no longer than 6 months[32] or that (ii) fall under the exceptions of Article 4 of the Cabinet Order and that are likely to harm the public or other interests if their presence or absence is made known.

73. The Supplementary Rule (2) provides that "*personal data received from the EU based on an adequacy decision is required to be handled as retained personal data irrespective of the period within which it is set to be deleted.*"

74. However, personal data falling under the exceptions of Article 4 of the Cabinet Order will not be required to be handled as retained personal data and that data subject rights will not apply.

75. Article 23 of the GDPR provides that, like Article 4 of the Cabinet Order, Union or Member State law to which the data controller/processor is subject to, may restrict the scope of the obligations applicable to him and the rights available to the data subject. This can be done by way of a legislative measure. These restrictions need to respect the essence of the fundamental right and freedoms and is a necessary and proportionate measure in a democratic society.

76. Regarding the substance of the exceptions provided for in Article 4 of the Cabinet Order, the EDPB has not been provided with sufficient documentation on these limitations or additional elements to clarify the scope of these provisions[33]. 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 provided to the EU data subjects.

77. **Due to lack of some relevant documents, the EDPB would also welcome reassurances by the European Commission, if restrictions to the rights of individuals (in particular, rights of access, rectification and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights.**

78. An essential requirement under the GDPR is that personal data are protected throughout their whole "life cycle".

79. Taking into account the fact that the Supplementary Rules only apply to personal data transferred from the EU, the EDPB would appreciate receiving further information about the practical implementation of these rules by PIHBOs, especially when these data are further communicated to another PIHBO after their first transmission to Japan.

80. The European Commission has clarified in recital 15 of its draft adequacy decision that PIHBOs receiving and/or further processing personal data from the EU will be under a legal obligation to comply with the Supplementary Rules and that in order to do so they will need to ensure that they can identify such personal data throughout their "life-cycle".

---

[31] Articles 27-30 of the APPI.

[32] Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order), put into effect May 30, 2017, Article 5.

[33] The EDPB has not been provided with the Supreme Court decisions referred to in recital 53 of the draft adequacy decision.

81. In its answers, The PPC[34]has explained that such identification will be made by using technical methods (tagging) or organisational methods (storing the data originating from the EU in a dedicated database).

82. In footnote 14 of its draft adequacy decision, the European Commission explains that PIHBOs must record the information on the origin of the EU data for as long as necessary in order to be able to comply with the Supplementary Rules. This is also enshrined in Article 26 (1), (3) and (4) of the APPI which states that a PIHBO is under the obligation to confirm and record the source of these data and all the circumstances surrounding the acquisition of these data.

83. However, the EDPB notes that Article 18 of the PPC Rules[35] specifies that the record keeping obligations of PIHBOs are limited to a maximum of three years for cases that fall outside the specific record keeping methods described in Article 16 of the PPC Rules (using a written document, electromagnetic record or microfilm). This is also stated by the European Commission in recital 71 of its draft adequacy decision: "*As specified in Article 18 of the PPC Rules, those records must be preserved for a period of one to three years, depending on the circumstances*".

84. Even if, as the European Commission states in footnote 14 of its draft adequacy decision, PIHBOs are not prohibited to keep records regarding the origin of the data for longer than three years, in order to be able to fulfil their obligations under Supplementary Rule (2), this is neither clearly reflected in the Japanese legislation nor in the Supplementary Rules. The EDPB considers that there is a risk that PIHBOs will in fact comply with Article 18 of the PPC Rules even when they process data originating from the EU. This is mainly because there is currently, to the understanding of the EDPB and based on available documents, no provision putting PIHBOs under such an obligation to comply with the Supplementary Rules instead. This would result in data transferred from the EU to no longer being protected by the additional protections included in the Supplementary Rules.

85. **The EDPB invites the European Commission to closely monitor the effective protection of personal data transferred from the EU to Japan based on the draft adequacy decision, throughout their whole life-cycle even though the Japanese legislation imposes a record keeping obligation of the origin of the data for a maximum of three years.**

3.1.2 Grounds for lawful and fair processing for legitimate purposes

86. According to the adequacy referential, in line with the GDPR, data must be processed in a lawful, fair and legitimate manner[36]. The legal basis, under which personal data may be lawfully, fairly and legitimately processed, should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including, for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.

87. Under the APPI, consent plays a central role in the Japanese data protection legal system. Consent is the central legal basis for the processing of personal data in Japan, and also one of the main legal basis for transfers of personal data from Japan to a third country. In addition, consent is required for an alteration of the purpose of the processing.

88. According to Supplementary Rule (3), the legal basis for the processing of personal data transferred from the EU to Japan will be the legal basis for which the data is transferred to Japan. If the PIHBO

[34] Annex III of the present Opinion.
[35] Enforcement Rules for the Act on the Protection of Personal Information (PPC Rules), put into effect May 30, 2017, Article 16.
[36] WP254, p.4.

wishes to process further these data for a different purpose he needs to obtain the consent of the data subject in advance.

89. The EDPB considers that the quality of consent, especially due to its central role in the Japanese legal framework, has to comply with the fundamental requirements of the notion of consent, i.e. according to EU law, a *"freely given, specific, informed and unambiguous indication of the data subject's wishes..."*. The data subject can withdraw such consent as an essential safeguard to ensure the free will of the data subject throughout the time[37]. The right to withdrawal, as a mandatory element of consent, appears to be missing in the Japanese legal framework. Indeed, according to the PPC guidelines[38] the withdrawal is merely "desirable" and conditional to the "characteristics, size and the status of the business activities".

3.1.3 The transparency principle

90. Based on Article 5 of the GDPR, transparency is a fundamental principle of the EU data protection system[39]. The adequacy referential explicitly names "transparency" as one of the content principles to be taken into account when evaluating the essentially equivalent level of protection provided for by a third country. The transparency and fairness principle strives to ensure that the data subject has control over his/her data and, for this purpose, information shall be provided to the data subject in a proactive manner as a rule. In the case of the Privacy Shield, the Article 29 Working Party[40] in their opinion 1/2016 made reference to Annex II, II 1 b of the Privacy Shield agreement (notice to the individual) and stated that, if the data is not collected directly, an organisation should notify the data subject "at the point the data is recorded by the Shield organisation" (section 2.2.1.a). Having the privacy policy publicly available is an additional criterion (see section 2.2.1.b). Hence, already under Directive 95/46/EC it was deemed necessary to directly inform the data subject.

91. A first concern is raised regarding the modality of information provided to the data subject under the APPI. According to Article 27 (1) of the APPI, a PIHBO is obliged to provide the information described in Article 27 (1) APPI by putting it "into a state where a principal can know". However, this wording does not make clear to what extent the PIHBO has to take positive measures to genuinely inform the data subject.

92. **The EDPB invites the Commission to clarify the meaning of the term "can know" and whether the APPI provides as a rule the obligation to genuinely inform data subjects.**

93. Moreover, according to the adequacy referential, restrictions to the information to be provided to the data subject may exist, similar to Article 23 GDPR. On a similar vein, Article 14 (5) of the GDPR provides for an exception to the right to be informed when the information is likely to render impossible or seriously impair the achievement of the processing. However, even in this case, the controller shall provide some sort of information as, for instance, by making "generalised" information publicly

[37] GDPR, Article 4(11). For more information see also relevant guidelines of the EDPB on consent WP259, 10 April 2018.

[38] Data Protection Legal and Technical Research and Analysis Consortium (DPC), An assessment of the level of protection of personal data provided under Japanese law, p. 46: "Further, from the viewpoint of protection of rights and interests of a principal such as consumers, it is desirable, in case of having received a demand from a principal for the retained personal data, to further respond to the principal's demand in such a way as stopping etc. of direct-mail sending or voluntarily fulfilling a utilisation cease etc. considering the characteristics, size and the status of the business activities".

[39] WP 254, chapter 3, point 7, p. 5; see also recital (39) GDPR.

[40] This Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The WP29 has now become the EDPB.

available. Moreover, when the risk ceases to exist the data subject shall be notified[41]. These aspects are important in order to ensure the fundamental principle of fairness.

94. Under Article 23 of the APPI, a PIHBO generally has to give in advance information to the data subject about providing his/her data to a third party either implicitly when obtaining his/her consent or explicitly by an opt-out notification. The EDPB understands that there is no notification to the data subject, informing him/her of the fact that his/her data are not retained personal data under the APPI because falling under the exceptions of Article 4 of the Cabinet Order. As a result, they will not be able to benefit from their rights in full. The data subjects are not informed in the cases of Article 18(4) APPI either.

95. **The EDPB acknowledges that the rights may be restricted for legitimate objectives pursued by the PIHBO and the state authorities. At the same time, the EDPB considers that there should be at least a general information upfront on the possibility of the restriction of the rights for the objectives referred to the law and that the data subject should be notified when the risks for which the information is restricted cease to exist.**

96. Finally, other aspects of transparency are developed further below. These refer to the risks the transfer to a third country entails[42] and the information on the logic of processing in the context of automated decision making, including profiling.[43]

3.1.4 Restrictions on onward transfers

97. The EDPB welcomes the efforts made by the Japanese authorities and the European Commission to enhance the level of protection for onward transfers in Supplementary Rule (4), which excludes that personal data transferred from the EU is further transferred to a third country on the basis of APEC-CBPRs. In addition, the EDPB recognises that in in recitals 177 and 184 of its new draft of the adequacy decision, the European Commission committed itself to suspend the adequacy decision when onward transfers no longer ensure the continuity of protection. However, the EDPB would like to raise two points regarding these transfers of EU personal data from Japan to third countries.

98. **The use of consent as a basis for data transfers from Japan to a third country in the Japanese legal system raises concerns as the EDPB considers that the information given to the EU data subject prior to consenting seems not to be comprehensive.**

99. Article 24 APPI prohibits the transfer of personal data to a third party outside the territory of Japan without the prior consent of the individual concerned. Supplementary Rule (4) stipulates that EU data subjects have to be provided with information on the circumstances surrounding the transfer necessary to make a decision on his/her consent.

100. The European Commission concludes in its draft adequacy decision that Supplementary Rule (4) secures a particular well informed consent of the EU data subject[44] as he/she will be advised of the fact that the data will be transferred abroad and of the specific country of destination. This would allow the data subject to assess the risk for privacy involved with the transfer.

---

[41] Tele2, Joined Cases C 203/15 and C 698/15, judgement of the Court, 21 December 2016, rec. 121 and Digital Rights Ireland, Joined Cases C-293/12 and C-594/12, judgement of the Court, 8 April 2014, rec. 54-62.
[42] See section 2.1.4.
[43] See section 2.1.6.
[44] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, Recital 76.

101. Under the transparency principle of the adequacy referential, a certain degree of fairness shall be ensured when informing individuals. In the context of onward transfers based on consent, the EDPB is of the opinion that to ensure such adequate degree of fairness data subjects should be explicitly informed about the possible risks of such transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards prior to consent. Such notice should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country[45]. For the EDPB the provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer[46].

102. Informed consent is also important regarding sectorial exclusions. The adequacy decision does not cover certain types of processing by certain bodies such as universities for the processing of personal data for academic purposes. The EDPB's concern here relates to the specific scenario of when data transferred from the EU under the adequacy decision – for example the HR data of Erasmus students in Japan – are then used for a different purpose falling out of the scope of the adequacy decision (e.g. research purposes), with the consent of the data subject, - and are therefore no longer covered by the additional protection provided by the Supplementary Rules.

103. The European Commission states in recital 38 of its draft adequacy decision that such a scenario will fall under the context of onward transfers and that, where this takes place, the PIHBO has to provide the data subject with all the necessary information before obtaining his/her consent, including that the personal information would not fall under the protection of the APPI rules.

104. Supplementary Rule (4) only requires the PIHBO to obtain the data subject's consent after having been provided with information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent.

105. **The EDPB invites the European Commission to ensure that the information to be provided to the data subject "on the circumstances surrounding the transfer" should include the information about the possible risks of transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards, or in the case of sectorial exclusions, of the absence of protections of the Supplementary Rules and of the APPI.**

106. **Onward transfers of personal data may occur to third countries, which become subject to a possible later Japanese adequacy decision.**

107. Without prejudice to the derogations set forth in Article 23 para 1 of the APPI, data initially transferred from the EU to Japan can be then transferred from Japan to a third country without consent in two cases:

- If the PIHBO and the third party recipient have together implemented measures providing a level of protection equivalent to the APPI read together with the Supplementary Rules by means of a contract, other forms of binding agreements or binding agreements within a corporate group[47].

[45] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.8.
[46] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.7.
[47] Supplementary Rule (4) (ii).

- If the third country has been recognised by the PPC under Article 24 of the APPI and Article 11 of the PPC Rules[48] as providing an equivalent level of protection to the one guaranteed in Japan.

108. The EDPB evaluates Article 24 APPI as the more specific rule, which contains a derogation from the general rule under Article 23 APPI. Therefore, the EDPB does not share the European Commission's assessment in the new last sentence of Recital 78 of the draft adequacy decision stating that even in those cases, the transfer to the third party remains subject to the requirement to obtain consent under Article 23 (1) of the APPI.

109. Pursuant to Article 11 (1) of the PPC Rules, an adequacy decision by the PPC requires substantive standards equivalent to the APPI whose implementation are ensured in the third country and which are effectively supervised by an independent enforcement authority. Moreover, the PPC may impose necessary conditions to protect the rights and interests of individuals in Japan, according to Article 11 (2) of the PPC Rules.

110. Supplementary Rule (4) states that EU personal data can be transferred to a third country subject to a Japanese adequacy decision without further restrictions. But Article 44 of the GDPR regulates that any transfer of personal data to a third country has to fulfil the conditions laid down in Chapter V of the GDPR including onward transfers from the third country to another third country. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer[49]. Although this interpretation is in principle also shared by the European Commission in its draft adequacy decision[50], it seems not to be completely followed. The European Commission has negotiated the prohibition of data originating from the EU being transferred to a third country on the basis of Asia Pacific Economic Cooperation (APEC) – Cross Border Privacy Rules (CBPRs). In the light of the comparative tool developed in 2014 under the framework of the EU Directive between BCR and CBPR showing the requirements of both systems, their convergences and differences (WP29 Opinion 02/2014), the EDPB has concerns about the use of CBPRs as an onward transfer tool for personal data transferred from the EU to countries outside of Japan.

111. In contrast, onward transfers of personal data transferred from the EU to Japan on the basis of a Japanese adequacy decision, seem to be accepted by the European Commission, without the possibility for the PPC to impose the Supplementary Rules as conditions to protect the rights and interests of EU individuals, if necessary. The EDPB deduces from Article 44 of the GDPR that the enhanced protection of data being transferred from the EU to Japan foreseen in the Supplementary Rules has always to be extended when personal data transferred from the EU to Japan is further transferred to a third country, if the data protection framework in that country is not recognised as essentially equivalent to the GDPR.

112. **Hence, the EDPB invites the European Commission to take over its monitoring role and to ensure the level of protection of EU data is maintained or to consider suspension of this adequacy decision if personal data transferred from the EU to Japan is further transferred to third countries subject to a**

[48] Enforcement Rules for the Act on the Protection of Personal Information, 30 May 2017. An English translation of the new Article 11 was communicated by the EU Commission to the EDPB, but this Article has not been published yet.
[49] WP 254, p.5.
[50] Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, Recital 75.

possible later Japanese adequacy decision, when these third countries have not been subject of a previous assessment or adequacy finding of the EU.

3.1.5 Direct marketing

113. According to Supplementary Rule (3), a PIHBO is prohibited from processing the data for the purpose of direct marketing if it has been transferred from the European Union for another purpose and the EU data subject has not given his or her consent to the change of the utilisation purpose.

114. According to the Adequacy referential where data are processed for the purposes of direct marketing, the data subject should be able to object without any charge from having his/her data processed for such purposes at any time. According to Article 16 of the APPI, a PIHBO is only allowed to process personal information if the data subject gives his or her consent. The withdrawal of consent could provide the same result as the privileged right to object to direct marketing.

115. The Japanese data protection framework does not provide a privileged right of objection and as explained above in the section on consent, withdrawal of consent under the PPC Guidelines is merely desirable and conditional and can therefore not be considered to equate to a right to object at any time as requested under the Adequacy referential. **The EDPB invites the European Commission to provide reassurances about the right to withdrawal of consent and to monitor cases regarding direct marketing.**

3.1.6 Automated decision making and profiling

116. According to the adequacy referential, decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. Therefore, every time automated decision making and profiling under the aforementioned circumstances is conducted, there has to be a legal ground for this.

117. In the European framework, the conditions for automated decision making include, for example, the need to obtain the explicit consent[51] of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. Furthermore, the law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved to correct inaccurate or incomplete information and to contest the decision where it has been adopted on an incorrect factual basis.

118. The Commission decision only refers to banking sector where sectoral rules[52] regarding automated decisions would apply. The Comprehensive Guidelines for Supervision over Major Banks mentioned in recital 93 of the draft adequacy decision indicate that the concerned individual has to be provided with specific explanations on the reasons for the rejection of a request to conclude a loan agreement.

119. The argumentations of the European Commission referring to the draft adequacy decision (Recital 94), that the absence of specific rules on automated decision making in the APPI is unlikely to affect the level of protection seems (for instance) do not to take into account the case in which an EU-transferred

[51] For critical remarks to the concept of consent in the Japanese data protection legal framework see: 2.1. General and 2.2.8. Direct marketing.

[52] These Sectoral Rules were not provided to the EDPB.

personal data is subsequently processed by another Japanese data controller (different from the original Japanese data importer).

120. It appears therefore, that there are no general rules applicable across sectors in Japan governing automated decision making and profiling.

121. **The EDPB invites the European Commission to monitor cases related to automated decision making and profiling.**

3.2 Procedural and enforcement mechanisms

122. Based on the criteria set in the adequacy referential, the EDPB has analysed the following aspects of the Japanese data protection and legal framework as covered under the draft adequacy decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance and a system of access to appropriate redress mechanisms equipping EU individuals with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.

123. Building on the parameters established by the CJEU in the Schrems case[53] and those outlined in recital 104 and Article 45 of the GDPR, the EDPB finds that, although a system consistent with the European one exists in Japan, this system may be difficult to access in practice for EU individuals, whose data will be transferred under this adequacy decision in light of the existence of language and institutional barriers.

124. The sections below will examine the above mentioned aspects of the Japanese framework before highlighting some recommendations for the Commission.

3.2.1 Competent independent Supervisory Authority

125. The PPC was established on the 1 January 2016 following the amendments of the APPI of 2015, replacing its predecessor – the Specific Personal Information Protection Commission (established in 2013 under the My Number Act). Although a young organization, since its establishment, the PPC has put considerable efforts into building the required infrastructure to accommodate the implementation of the amended APPI. Noticeable among these are the establishment of the PPC's rules, the PPC Guidelines to give guidance to PIHBOs on the interpretation of the APPI, the publication of a PPC Q&A[54] document and the setting up of a helpline to advise business operators and citizens on data protection provisions as well as of a mediation service to handle complaints.

126. The establishment and functioning of the PPC is regulated in chapter V of the APPI. Although the PPC falls within the jurisdiction of the Prime Minister, article 62 mandates that the PPC exercises its function independently. The EDPB welcomes the clarification made by the European Commission in the amended draft of the adequacy decision circulated on 13 November 2018 to further describe the degree to which the PPC is free from internal and external influences.

3.2.2 The data protection system must ensure a good level of compliance

127. The draft adequacy decision undertakes a comprehensive examination of the powers that the PPC is equipped with under Articles 40, 41 and 42 of the APPI to ensure the monitoring and enforcement of the legislation. Article 40 empowers the PPC to request PIHBOs to submit reports and documentation relating to processing operations as well as to carry out on-site inspections. Under Article 42, the PPC has the power – when recognising that it is necessary to protect individual rights or where finding a

[53] Case 362/14 (2015) Maximilian Schrems v Data Protection Commissioner, (para. 73 and 74).
[54] This document was not provided by the European Commission to the EDPB in English.

violation of the provisions of the law – to issue recommendations and, those failing, orders to PIHBOs to suspend the act of violation or take necessary measures to rectify the violation.

128. In October 2018, the PPC took one of its first actions under article 41 of the amended APPI and issued 'guidance' to a PIHBO, advising the company to strengthen its' security measures and to effectively supervise applications providers whilst giving clear and easy to understand explanations to users on how their personal information is used, and obtain consent beforehand when the information is shared with a third party as well as respond properly to users' request for erasure of their information. In the answers provided to the EDPB[55], PPC officials advised that the company has announced it will cooperate and that, when the company fail to do so, it will render the company with a 'recommendation' under Article 42(1) of the APPI.

129. The investigation conducted by the PPC on the above mentioned PIHBO is a very positive indicator of the Japanese supervisory authority's efforts to ensure a good level of compliance in the country.

130. Although there are improvements in respect to the framework in place prior to the 2015 amendments, the EDPB notices that the PPC has fewer powers than European DPA under the GDPR, especially in relation to **enforcement**. Administrative fines[56], for example, are quite mild. The European Commission's decision emphasises in recital 108 that, in cases of non-compliance or some violations of the APPI, criminal sanctions are in place and that the PPC Chair may forward cases to the public prosecutor. However, the European Commission's decision does not account for the fact that public prosecution in Japan is discretional and may sometimes be subject to lengthy review processes[57]. In addition, the penalty of imprisonment (with or without labour) associated with violations of the APPI pursuant the provisions in Chapter VII may be difficult to execute because directed at natural persons and, in any case, not punishing the PIHBO as a legal entity failing to exercise its accountability obligations.

131. **In light of the above, the EDPB invites the European Commission to closely monitor the effectiveness of sanctions and relevant remedies in the Japanese data protection system.**

3.2.3 The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

132. The PPC provides extensive information and guidelines on its website aimed at raising awareness among PIHBOs in relation to their obligations and responsibilities under the data protection framework as well as a Helpline to provide information and support to Japanese citizens regarding their individual rights under the APPI. The website has also a section, called the 'Children's room', explicitly aimed at a children's and young people audience. The EDPB observes that this information – along with the Helpline support, guidance and Q&A documentations – is available in Japanese[58]. Therefore, the EDPB strongly believes, it would be beneficial if the PPC could provide a dedicated page on the English version of its website aimed at providing information about their individual rights under the Japanese

---

[55] Annex III.

[56] These are provided in Chapter VII of the APPI. The maximum penalty is provided by art. 83 (provision or use by stealth of a personal information database for own or a third party's illegal profit) and is equivalent to either a year's imprisonment with work or a fine not exceeding 500,000 yen (roughly EUR 3900). According to the explanations provided by the Commission, fines are cumulative per infringement. Although this may be the case, the EDPB observes that, even if cumulative fines are applied, the total amount is likely to remain considerably low compared to European standards.

[65] Oda H., Japanese Law, Oxford University Press (III edition), 2009: 439 – 440.

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

data protection framework and under the Supplementary Rules to EU individuals whose data will be transferred to Japan under the European Commission's adequacy decision.

133. The EDPB welcomes the clarification made by the European Commission in recital 104 of the amended draft adequacy decision circulated on 13 November 2018 regarding the mediation service managed by the PPC pursuant Article 61(ii) of the APPI. However, the EDPB would like to raise three points in relation to this. Firstly, the mediation service is not publicized on the English version of the PPC's website. Secondly, the service is accessible only via phone and available in Japanese. Finally, mediation is merely a facilitative process not leading to a binding agreement between the parties which has implications for the effectiveness of the redress options available to data subjects[59].

134. Finally, the EDPB notices that the draft adequacy decision places emphasis on the remedies available through civil law action as well as criminal proceedings, but does not acknowledge the existence of **institutional barriers to litigation** in Japan such as legal costs (legal fees are split equally between plaintiff and defendant, regardless of which party wins the proceedings[60]), dearth of lawyers in the country[61], the fact that foreign lawyers are not allowed to practice domestic law as well as the burden of proof requirement under Tort Law. The EDPB fears that these factors may – in practice – hinder individuals' access to justice and jeopardise their right to pursue legal remedies rapidly and without bearing prohibitive costs.

135. In light of the above, **the EDPB is concerned that there is a risk that EU individuals may have difficulties accessing administrative and judicial redress** and, therefore, would welcome if the European Commission could discuss with the PPC the possibility of setting up an online service, at least in English, **aimed at providing support to, and handle complaints of[62], EU individuals**. In addition, the EDPB would welcome the possibility of allowing EU DPAs to act as intermediaries for EU data subject complaints with organisations operating in Japan and the PPC.

4 ON THE ACCESS BY PUBLIC AUTHORITIES TO THE DATA TRANSFERRED TO JAPAN

136. The intention of the COM is to recognise, through the adequacy decision, that "Japan ensures an adequate level of protection for personal data transferred from the European Union to personal information handling business operators in Japan", as stated in Art. 1 of the draft adequacy decision. In line with Art. 45 (2) GDPR, the COM has also analysed the limitations and safeguards as regards access to personal data by public authorities. This chapter focuses on the assessment of the access to personal data by law enforcement authorities and by other government entities for the purpose of national security. The analysis of the EDPB is based on the draft adequacy decision, its Annex II, in which the Japanese government provides an overview of the relevant legal framework, and the Japanese legal texts, to the extent they were provided by the COM. Therefore, in the specific context of this assessment, the EDPB has taken into account elements concerning Japanese laws which are not

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; and Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).
[60] Wagatsuma (2012), 'Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure' in Reimann (ed.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11, pp. 195 – 200.
[61] According to the latest figures, the number of lawyers in Japan is 38,980 (roughly 290 layers per one million people [Japan Federation of Bar Association] (2017), White Paper on Attorneys: p. 8 – 9.
[62] Similar to the one envisaged in Annex II of this adequacy decision for complaints from EU residents regarding access to their data by Japanese public authorities.

part of the findings by the European Commission, but that are relevant to assess the conditions and safeguards under which Japanese public authorities are allowed to access personal data transferred from the European Union.

4.1 Law enforcement access to data

4.1.1 Procedures for accessing data in the field of criminal law

137. The draft adequacy decision presents three ways foreseen under Japanese law for law enforcement authorities to access data in Japan:

4.1.1.1 Access requests with a court warrant

138. The draft adequacy decision states that for government access in Japan, and especially for criminal law enforcement authorities to request access to electronic evidence in the context of criminal investigations, they always need to have a warrant, unless they use the voluntary disclosure procedure – see below.

4.1.1.1.1 Requirement of "adequate cause", necessity and proportionality of the warrants

139. The EDPB acknowledges that under the Japanese constitution any collection of personal data by compulsory means must be based on a court warrant. More specifically, the draft adequacy decision indicates that in all cases of "searches and seizures", court warrants have to be issued for "adequate cause", which the Supreme Court considers only exists where the individual concerned (suspect or accused) is considered to have committed an offence and the search and seizure is necessary for the criminal investigation. The COM here references the Supreme Court judgment of 18 March 1969, case N. 100 (1968(Shi)).). The EDPB recalls that under the CJEU's case law[63] only a court, and not prosecutors for instance, can authorize the collection of traffic and location data in particular.

140. Also in light of the CJEU jurisprudence, according to which access to data may be subject to a warrant, as in Tele2, the EDPB regrets that no additional information were provided in order to assess how the criteria for assessing the necessity of a warrant – gravity of the offense and how it was committed ; value and importance of the seized materials as evidence ; probability of concealment or destruction of seized materials ; extent of the disadvantages caused by a seizure ; other related conditions – and the concept of "adequate cause" derived from the Constitution are applied in practice. Therefore, the EDPB invites the Commission to monitor if the issuing of warrants meets the criteria set out by the CJEU in practice.

4.1.1.1.2 Types of crimes for which warrants can be issued

141. The warrant procedure applies only whenever a "compulsory investigation" is carried out. In principle, these warrants can only be issued in cases where a violation of law has occurred. In this respect, the EDPB notes the recently adopted "Act on Punishment of Organized Crimes and Control of Crime Proceeds" on 15 June 2017 in the context of adherence of Japan to the UN international Convention on Transnational Crime (UNTOC)[64]. In the absence of an English available version of this legislation, and given the requirement under EU law that some data are collected only in the context of investigation, detection or prosecution of serious crimes[65], as well as given concerns expressed by several commentators, including UN Special Rapporteur Joseph Cannataci[66], concerning the wide scope of application, and which relies on a definition of "organized criminal group" reportedly vague

[63] See cases 203/15 and C 293/12 and C 594/12 of the CJEU.
[64] See: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .
[65] See joint cases C 293/12 and C 594/12 and case C 203/15.
[66] UN Special rapporteur on the right to privacy, as well as Graham Greenleaf, UNSW Law Researcher.

and too broad, the EDPB is not in a position to conclude that access to electronic evidence under the relevant Japanese legislation is limited to the thresholds provided by EU law.

142. It has also to be noted that for some types of offences, the Prefectural Police is competent and that they have their specific police ordinances. The internal rules applicable to the Prefectural police were not available to the EDPB.

143. According to the draft Adequacy decision, the collection of electronic information in the area of criminal law enforcement falls under the responsibility of the Prefectural Police.

4.1.1.2 Wiretapping warrants

144. Annex II of the draft adequacy indicates that the Act on Wiretapping for Criminal Investigation provides for specificities for the interception of communications. This legislation was provided very late which did not allow for an in-depth analysis. Therefore, although many safeguards seem to be provided within this legal framework, the EDPB is not in a position to assess whether the conditions provided in this piece of legislation are surrounded by guarantees substantially equivalent to those required in the EU both by the Charter as interpreted by the CJEU and by the ECHR as interpreted by the Strasbourg Court.

4.1.1.3 The "voluntary disclosure" procedure based on enquiry sheet

145. This non-compulsory form of cooperation allows public authorities to ask controllers (except telecommunications carriers) to provide them with data they have. Non-compliance with the request cannot be enforced. It remains unclear which authorities can use this type of procedure, but it appears limited to those investigating crimes.

4.1.1.3.1 Conditions to issue "enquiry sheets"

146. The EDPB acknowledges that the Japanese Supreme Court, by reference to the Constitution, has framed limitations to the use "voluntary disclosures"[67]. It appears from the draft adequacy decision that concretely a "voluntary disclosure" may only be asked by the competent authorities through the issuance of an "enquiry sheet". Sending such an "enquiry sheet" is said to be permissible only as part of a criminal investigation, and thus to always presuppose a concrete suspicion of an already committed crime. Such investigations are generally carried out by the Prefectural Police, where the limitations pursuant to Article 2(2) of the Police Law apply, which means it should be relevant for the Police activities. However, the EDPB seeks further clarification as to the concrete contours of the criteria allowing to issue an enquiry sheet (such as case law illustrating the application of these criteria), and the relationship between the voluntary disclosure procedure and the seizure of data on the basis of a warrant. Indeed, it appears that even where data could not be obtained through the voluntary procedure, they could still be obtained with a warrant if indispensable for the investigative authorities[68].

4.1.1.3.2 Available case law on the limitations to the use of voluntary disclosure

147. The cases quoted in the draft adequacy decision[69] to illustrate limitations to the use of voluntary disclosure procedures relate to cases, where the accused person was either photographed or filmed in the public space by the police directly, and therefore give limited indications as to situations where the competent authorities can ask a controller to disclose data, in particular with regards to the criteria listed under Annex II concerning the "appropriateness of methods", which seems to concern the

[67] See Annex II page 8.
[68] See Annex II page 7.
[69] See Annex II page 8 – two Supreme Court decisions of December 24th, 1969 (1965 (A) No.1187) and April 15th, 2008 (2007 (A) No.839).

assessment of whether voluntary investigation is "appropriate" or reasonable in order to achieve the purpose of the investigation. The same can be said concerning the general criteria of "whether it can be considered reasonable in accordance with socially accepted conventions" to assess the legality of voluntary investigations. Furthermore, the National Police Agency, which is the federal authority in charge of all matters concerning the criminal police, issued instructions to the Prefectural Police on the "proper use if written inquiries in investigative matters". Among others, the chief investigator must receive internal approval from a high-ranking official. The EDPB has no information if these instructions are binding. Nevertheless the EDPB states, that the use of this procedure has to be proportionate or necessary.

4.1.1.3.3 Rights and obligations of the controllers in the context of voluntary disclosure

148. In addition, it is for the controllers to consent to provide data (but there appears to be no obligation on their part to seek the consent of data subjects or to inform them), where these requests do not conflict with other legal obligations (such as confidentiality obligations). The report provided by the Commission seems to indicate that after a high rate of compliance, controllers have started taking into account data protection of their customers' and thus have started answering less frequently to these requests.

149. It also remains unclear if controllers have any incentive to comply with the requests (for instance, if they have an advantage when complying, or if they are exempted from prosecution, etc). In particular, no mention is made of any principle such as the "non-self-incrimination principle".

150. The EDPB would welcome additional information, if available, figures on the number and types of requests, as well as on the answers provided by the controllers requested. In the absence of case law and figures, the EDPB invites the Commission to monitor the efficiency and concrete application of this procedure in practice

151. However, the EDPB lacks case law and figures on this procedure to establish these elements. Consequently, the EDPB is not in a position to provide an assessment concerning the efficiency and concrete application of this procedure without further elements concerning the practice.

4.1.1.4 Conclusion on procedures for accessing data for law enforcement purposes

152. As a conclusion, the EDPB acknowledges that the principle according to which personal data can be compulsorily accessed by the competent authorities only when necessary and proportionate to the purpose, and on the basis of a warrant, corresponds to the main essential guarantees provided under EU and ECHR law. Following the findings above, the EDPB asks the Commission to monitor the scope of these measures, the scope of the voluntary disclosure procedure and the application of these principle by the Prefectural Police and by the Courts in the relevant case law and to monitor too, if the Japanese legal framework is providing the essential guarantees drawn by the CJEU on the basis of the Charter and the ECHR on the basis of the Convention.

4.1.2 Oversight in the field of criminal law

153. The draft adequacy decision as well as the Annex II present four types of oversights conducted on the police, ministries and public agencies.

4.1.2.1 Judicial oversight

4.1.2.1.1 In cases where electronic information is collected by compulsory means (search and seizure)

154. According to the draft adequacy decision, in all cases where electronic information is collected by compulsory means (search and seizure), the police has to obtain a prior court warrant. However, there

is an exception to this rule. [70]. Indeed, article 220 (1) of the Code of Criminal Procedure allows a public prosecutor, its assistant or a judicial police official, when they are arresting a suspect to search or seize electronic information on the spot of the arrest. In this situation, there is a possibility for those information to be excluded as evidence by a judge.

155. The EDPB is mindful that similar exceptions also exist under EU law. It notes that there is not always a judicial control in cases where electronic information is collected by compulsory means, as it is stipulated in the draft adequacy decision. In this context, the EDPB recalls the jurisprudence of the ECHR on judicial a posteriori checks.[71]

4.1.2.1.2 In the case of requests for voluntary disclosure

156. According to the draft adequacy decision, in the case of the requests for voluntary disclosure, there is no ex ante control by a judge. In such case, the Prefectural Police operates under the supervision of the public prosecutor. The draft adequacy decision mentions articles 192 (1) and 246 on the mutual cooperation and coordination of the prosecutors, Prefectural Public Safety Commission and Judicial Police Officials and exchange of information between them. It also refers to article 193 (1) according to which public prosecutor may give necessary instruction to judicial police as well as setting standards for fair investigation. Finally, it mentions article 194 on the disciplinary actions against judicial police for not respecting the public prosecutors taken by the National or Prefectural Public Safety Commission.

157. The EDPB acknowledges the establishment of the previous measures and the oversight conducted by National and Prefectural Public Safety Commission on the judicial police (see below).

4.1.2.2 Oversight by the Public Safety Commissions of the police

158. According to the Annex II of the draft adequacy decision, two types of commissions are exerting an oversight of the police. Both aim at securing democratic management and political neutrality of the police administration.

4.1.2.2.1 Oversight conducted by the National Public Safety Commission

159. Annex II of the draft adequacy decision mentioned the oversight conducted by the National Public Safety Commission on the NPA. The Police Law gives a list of the duties of the Commission from which emanates its supervisory powers (see Article 5).

160. According to Article 4 of the Police Law, the National Public Safety Commission is established under the jurisdiction of the Prime Minister and is composed of a chairman and five members. Article 7 establishes some limitations to the appointment of the members of the Commission. The term of Office of Members of the Commission is five years and may be re-conducted one time only, as prescribed in Article 8. Furthermore, the Diet, appears to have a strong power over the appointment and the dismissal of the Commission's member which ensure the independence of the National Public Safety Commission.

161. Such legal provisions enhance the political neutrality of the National Public Safety Commission.

4.1.2.2.2 Oversight conducted by Prefectural Public Safety Commissions

162. The Prefectural Police is subject to the oversight of the Prefectural Public Safety Commissions established in each prefecture. According to Articles 2 and 36 (2) of the Police Law, the Prefectural Public Safety Commissions are responsible for "the protection of rights and freedom of an individual". Article 38 as well as Article 42 of the Police Law list the duties of the Prefectural Public Safety

[70] See Annex II.
[71] ECHR, Modestou v. Greece, N° 51693/13.

Commissions. Those Commissions also aim at securing democratic management and political neutrality of the police administration as stated in Article 43 (2) by issuing to the Prefectural Police individual cases when they consider this necessary in the context of an inspection of the activities of the Prefectural Police or misconduct of its personnel.

163. However, it is unclear whether those Commissions have other powers than the inspection of police's behavior. The EDPB is wondering whether the term "misconduct" is including illegal access of data and, in such a case, whether those Commissions are able to order the deletion of data or not.

164. Regarding the neutrality and the independence of those Commissions, as stated in the draft adequacy decision[72], Prefectural Public Safety Commissions are established under the jurisdiction of the prefectural governor who has to appoint members of the Commission with the consent of the prefectural assembly. Members of the Prefectural Public Safety Commission have a three years term and may be re-appointed up to two times. Article 39 of the Police Law enounced limitations concerning the appointment of the members. The draft adequacy decision also mentions the oversight of the Prefectural Police by local assembly, making reference of Article 100 of the Local Autonomy Act. However, this act was not provided to the EDPB[73].

165. Furthermore, according to Article 42 (2) and (3) of the Police Law, "No member of the Commission shall become concurrently a member of the assembly or the personnel in full-time service of local public entities or be engaged in part-time service prescribed in the provision of paragraph 1, Article 28 (5) of the Local Public Service Law.

166. According to the elements stated above and considering the collaboration between Prefectural Public Safety Commissions and National Public Safety Commission, the EDPB agrees with the draft adequacy decision and welcomes the neutrality and the independence of the members of the Prefectural Public Safety Commissions. The EDPB understands that Prefectural Safety Commissions only have a power to investigate police's behavior and do not have other supervisory powers, including the deletion of data collected by the prefectural police. Therefore, it appears that further clarification is needed as to whether the oversight conducted by Prefectural Public Safety Commissions is sufficient according the standards established under EU law.

4.1.2.2.3 Oversight conducted by the Diet

167. The draft adequacy decision[74] and the Annex II[75] are providing some information about the oversight conducted by the Diet in relation to the government, including with respect to the lawfulness of information collection of data by the police. Indeed, both mention the Article 62 of the Constitution according to which, the Diet may request the production of documents and the testimony of witnesses. Both are also mentioning legal provisions from the Diet Law, especially Article 104, concerning the powers of the Diet as well as Article 74 on the submission of written inquiries, which have to be answered by the Cabinet in writing within seven days as prescribed in Article 75. The draft adequacy decision also adds "The Diet's role in supervising the executive is supported by reporting obligations, for instance pursuant to Article 29 of the Wiretapping Act".

168. The EDPB acknowledges the implication of the Diet in the oversight of the government and the police regarding the lawfulness of data collection.

---

[72] See draft adequacy decision p. 31.
[73] See draft adequacy decision p. 33.
[74] See draft adequacy decision p. 30.
[75] See Annex II, p. 12.

4.1.2.2.4 Oversight conducted by the executive

169. According to the Annex II of the draft adequacy, on the one hand, the Minister or Head of each ministry or agency has the authority of oversight and enforcement based on the APPIHAO[76]. On the other hand, the Minister of Internal Affairs and Communications (MIC) has an investigative power concerning the enforcement of the APPIHAO by all other ministries, including the Minister of Justice for the Police as mentioned in the draft adequacy decision[77].

170. The Minister may request the head of an administrative organ to submit materials and explanations regarding the handling of personal information by the concerned administrative organ based on Article 50 of the APPIHAO. It may request a revision of the measures when it is suspected that a violation or inappropriate operation of the Act has occurred as well as issuing opinions concerning the handling of personal information by the concerned Administrative Organ according to Articles 50 and 51 of the APPIHAO.

171. The draft adequacy decision and the Annex II are also mentioning the establishment of 51 comprehensive information centres which are "ensuring the smooth implementation of this Act" according to Article 47 of the APPIHAO. The EDPB notes that the APPIHAO does not explain further the role and powers of those information centres but the draft adequacy decision provides some precisions.

172. Therefore, the EDPB welcomes the fact that there is an executive oversight on the respect of the APPIHAO on Ministries and administrative organs by the MIC.

173. As a conclusion, EU laws and the ECHR, in the jurisprudence of their respective Courts, are establishing standards and guarantees according to which the oversight has to be complete, neutral and independent. The EDPB notes that the PPC does not have supervisory powers in matters related to law enforcement. Furthermore, if the oversight conducted by the Diet, the National and Prefectural Safety Commission appears to be neutral and independent, further clarification is needed about the supervisory powers of the Prefectural Public Safety Commissions.

4.1.3 Redress in the field of criminal law

174. The draft adequacy decision, complemented by Annex II, presents several avenues through which individuals can bring their complaints, both before independent authorities and before judges.

175. These avenues and the core elements of these procedures stemming from the available documentation are presented here after, following a brief overview of the available rights to clarify what data subjects can expect from public authorities in the context of data processing in the field of criminal procedures.

4.1.3.1 Available rights of data subjects in the context of criminal procedures

176. In order to obtain redress, data subjects need to have rights under the law to be able to claim they were not respected. Therefore, the EDPB also assessed the available rights in the context of criminal procedures presented in the draft adequacy decision.

[76] See Annex II p. 10.
[77] See Annex II p. 11.

4.1.3.1.1 General limitations to the rights of data subjects under the APPIHAO

177. In its draft adequacy decision, the COM refers to and relies on general data protection principles which public authorities have to respect, once they have collected personal data. These principles are also further outlined in the Annex II so that the EDPB has decided to also comment on them.

178. Concerning available rights, the EDPB notes that, according to Annex II of the draft Adequacy decision, some of the general rights provided to data subjects in the context of data processed by Administrative organs, remain available also in the context of criminal investigations. However, additional limitations with regard to the collection and further handling of personal information in this context also follow from the APPIHAO itself.

179. These limitations, which also appear to apply both in the context of data collected on the basis of a warrant as well as on the basis of an enquiry sheet in the context of voluntary disclosure, raise questions concerning several aspects.

180. Concerning the principle of purpose limitation, although in principle administrative organs are required to specify the purpose for which they retain personal data, and shall not retain them beyond the scope necessary for the achievement of the purpose of use specified, they can change the purpose if it is "what can reasonably be considered as appropriately relevant for the original purpose".

181. The APPIHAO also provides for the principle of non-disclosure, according to which an employee shall not disclose the acquired personal information to another person without a justifiable ground or use such information for an unjust purpose. However, no additional information is provided concerning the interpretation of what "justifiable ground" or "unjust purpose" could cover, so that further clarification would be necessary for the assessment.

182. Article 8(1) of the APPIHAO also lays down the prohibition to use or disclose data "except as otherwise provided by laws and regulations". Nevertheless, although this provision is not in principle contrary to the level of protection afforded under EU law, the EDPB lacks additional elements concerning the extent to which any supervision or checks is exercised when disclosure is provided by laws or regulations. In addition, under Article 8(2), additional exceptions apply to this rule where "such exceptional disclosure is not likely to cause unjust harm to the rights and interests of the data subject or a third party". Without any further elements on this point, this exception, which relies on the unclear notion of "unjust" harm, needs further clarification, if it is narrow enough.

183. Lastly, Article 9 of the APPIHAO provides for additional restrictions on the purpose or method of use or any other restrictions, to be imposed by the head of an administrative organ where retained personal information is provided to another person. As the notions of "any other necessary restrictions" and "provided to another person" are very broad, these additional restrictions to the rights of data subjects raise concerns without further clarifications on the scope of this provision.

184. While the EDPB is fully aware that access rights and other data protection principles are also limited in criminal proceedings under EU law, additional safeguards are provided when such limitations are foreseen, including in terms of supervision, oversight and redress. In the absence of sufficient case law on these limitations or additional elements to clarify the scope of these provisions, 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.

4.1.3.1.2 Additional limitations to the rights of the APPIHAO deriving from the Code of Criminal Procedure and the Prefectural Police ordinances

185. The EDPB notes that although the APPIHAO seems to be applicable to all processing by administrative organs in Japan, some important limitations to the rights of data subjects derive from specific legislations. In particular, Article 53 (2) of the Code of Criminal Procedure[78] provides that "personal information recorded in documents relating to trials and seized articles" are excluded from the scope of application of the individual rights in Chapter IV of the APPIHAO. Concretely, the EDPB therefore understands that in the context of criminal procedures, data subjects do not benefit from the rights to information, access, rectification or erasure for personal data recorded in documents relating to trials and seized articles.

186. With regards to these limitations, the EDPB understands that they apply in the context of data collected on the basis of warrants, as well as in the context of data collected under the voluntary disclosure through enquiry sheets (see below). Indeed, the legal basis of the two procedures to access data (through a warrant and through an enquiry sheet) being provided in the code of criminal procedure, Article 53-2 of this code appears to apply to both types of collection. However, as Article 53-2 refers to the articles "seized" it could be clarified whether the limitations to the rights foreseen under this provision do apply also in the context of voluntary disclosure.

187. The EDPB regrets not to be provided with the ordinances of the Prefectural Police, which are said to be protecting personal information, rights and obligations equivalent to the APPIHAO. Given both the unclarities regarding the interpretation of the APPIHAO and the unavailability of the Prefectural Police ordinances, the EDPB wonders, if the granted rights to the individuals in this context, and the additional oversight and/or redress mechanisms are sufficient to compensate the absence of rights.

4.1.3.2 Redress through independent authorities redress

4.1.3.2.1 Administrative redress

188. The EDPB notes that the administrative organs collecting data, such as the Prefectural Police, are competent to deal with requests stemming from individuals concerning their – limited – rights with regards to their data collected as part of criminal investigations (see above concerning the rights available), which appear to include both the collection of data based on a warrant and on enquiry sheets. Concretely, these rights seem to be limited to general principles, such as the necessity of data retention, in connection with the purpose (see Article 3.1 APPIHAO), the purpose limitation principle (Article 4) or the accuracy of the data (Article 5), while individual rights such as the right to information, access, rectification or erasure are excluded for personal data recorded in documents relating to trials and seized articles[79]. Although these organs cannot be considered as independent and therefore as providing independent redress or oversight, the EDPB welcomes this avenue. However, it stresses that complaints filed in this context remain limited to very few rights of the data subjects given the limitations of rights provided by the APPIHAO.

189. Furthermore, as "personal information recorded in documents relating to trials and seized articles" are excluded from the scope of application of the individual rights in Chapter IV of the APPIHAO pursuant to Articles 53-2 of the Code of Criminal Procedure, the possibilities to request access to personal information are also limited to the procedures foreseen under other provisions of this Code of Criminal Procedure. It seems that only victims, suspected or accused persons can act in this context, and still,

[78] Available here http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 and quoted in Annex II of the draft adequacy decision, footnote 25.

[79] See supra concerning the limitations to APPIHAO and in particular see article 53-2 of the Code of Criminal Procedure (not provided but quoted in annex II of the draft adequacy decision, footnote 25).

depending on the stage of the criminal procedure. Therefore, the EDPB is concerned that no general right to access and/or rectify or delete information is available to data subjects under Japanese law in the context of criminal procedure, and that all redress avenues available imply to be either a victim (in which case the person would probably know that his/her data were collected) or a suspect or accused person, or the demonstration of a damage, while data subjects should also have the right to have access to their data and possibly to have their data rectified or deleted when they did not suffer any damage (yet possibly) and/or when they are neither a victim, a suspect or an accused person, but witnesses for instance.

4.1.3.2.2 Administrative redress through the Prefectural Public Safety Commissions

190. In addition, the Prefectural Public Safety Commissions appear to be competent to deal with complaints. Based on Article 79 of the Police law referred to in the draft adequacy decision, individuals can complaint against any illegal or improper behaviour of an agent in the execution of his/her duties.

191. The EDPB seeks clarification whether any "illegal" processing of personal data qualifies for an "illegal or improper behaviour of an agent" and on the demonstration of a disadvantage which seems required from the data subject. Indeed, the notice issued by the NPA to the Police and Prefectural Public Safety Commissions on the proper handling of complaints regarding the execution of duties by police officers limit the complaints to concrete claims concerning "correction for any specific disadvantage that has been inflicted as the result of an illegal or inappropriate behaviour, or failure to take a necessary action, by a police officer in his/her execution of duty" and the possibility to "file grievance/discontent about inappropriate mode of duty execution by a police officer". It is expressly clarified that "complaints on non-performance of a police officer concerning any matter that is not considered to fall under a police officer's duty, and also those expressing a general opinion or a proposal, not directly affecting the complaining party itself, shall be excluded".

192. Concerning the procedural requirements to file a complaint, although they have to be filed in writing, the EDPB notes that assistance for writing the complaint is provided in this context under Japanese law, including for foreigners. In addition, the Japanese government seems to have also entrusted the PPC with the duty to provide assistance to EU data subjects to handle and resolve complaints in this field, which the EDPB welcomes. The EDPB underlines that in its understanding, in this context, the PPC will only act as a point of contact between the EU data subjects and the competent authorities in Japan.

193. The results of the Prefectural Public Safety Commission following a complaint shall not be noticed in cases listed in Article 79-2 of the Police Act, which includes the case where the current "resident of the complainant is unknown". The EDPB acknowledges that the reference to the resident does not imply that in all cases EU data subjects would therefore be excluded from the notification of the results of their complaints on the ground they are not residing in Japan.

4.1.3.2.3 Ad Hoc mechanism implying the PPC

194. In view of the findings described above, The EDPB welcomes that the Japanese government and the EU Commission have agreed on an additional redress mechanism providing EU individuals with an additional avenue for redress in Japan through which individuals can also seek redress against unlawful or improper investigations by public authorities. The EDPB also notes and welcomes that the requests can be lodged with the PPC, rather than with another government official, thereby extending the scope of competence of the PPC to the area of law enforcement and national security.

195. The focus of the EDPB, when analysing the new mechanism, has been to understand the powers the PPC has in this context.

196. Even though the language is not entirely clear, the EDPB understands that the additional redress mechanism does not require "standing" in the meaning that the requestor is not required to show that her personal data is likely to have been subjected to surveillance by a Japanese authority. The EDPB would still like to request confirmation by the Commission.

197. In line with its assessment of the Ombudsperson mechanism, created under the Privacy Shield, the EDPB stresses the need for effective powers of the addressee of the request, in this case the PPC, in order to consider the redress mechanism as essentially equivalent to an effective remedy in the meaning of Art. 47 of the Charta on Fundamental Rights.

198. When explaining the redress mechanism, the Japanese government refers to Art. 6, 61 (ii) and 80 APPI and lays out these powers in Annex II. It is the understanding of the EDPB that the procedure as described in Annex II specifies or extends the powers of the PPC, as the language in Art. 6, 61 (ii) and 80 APPI is rather vague and general. To the extent Annex II specifies or extends the powers of the PPC, the EDPB would like to ask for clarification that the other agencies of the Japanese government are bound by them.

199. On the basis of the procedure in Annex II, the EDPB notes that the competent public authorities in Japan are required to cooperate with the PPC, "including by providing them with the necessary information and relevant material, so that the PPC can evaluate whether the collection or the subsequent use of personal information has taken place in compliance with the applicable rules". For the assessment of the effectiveness of the system, it is thus important to refer again to the powers that those competent authorities have with which the PPC cooperates. It is the understanding of the EDPB that those powers would not be extended through the reassurances in Annex II.

200. The EDPB also notes that, if a violation of the rules has been identified, "the cooperation by the concerned public authorities with the PPC includes the obligation to remedy the violation", which expressly includes the deletion of the data collected in violation of the applicable rules. The EDPB understands that the obligations of the competent authority stem from the "cooperation with the PPC", rather than from a decision by the PPC.

201. Finally, the PPC will inform the requestor of the "outcome of the evaluation, including any corrective action taken where applicable." In addition, the PPC will inform the requestor about the "possibility of seeking a confirmation of the outcome from the competent public authority and about the authority to which such a request for confirmation shall be made."

202. In addition, the PPC has committed to assist the requestor with bringing further action under Japanese law, if the requestor is dissatisfied with the outcome of the procedure.

203. In light of the need to have an effective redress mechanism essentially equivalent to the EU standards, the EDPB nevertheless wonders if the PPC has any specific powers other than evaluating whether the collection or the subsequent use of personal information has taken place in compliance with the applicable rules and calling on the competent authorities to use their respective powers and to deal with complaints forwarded to them by the PPC. Should the PPC only act as a contact point for the EU individuals, the EDPB would consider this as insufficient to provide for an effective redress mechanism essentially equivalent to the EU standards. The EDPB thus calls on the Commission to provide clarifications on the points mentioned in this sub-chapter, in particular on whether and how the mechanism extends the obligations of competent authorities, how they are bound by it, and how the PPC can effectively ensure compliance and not only acting as a contact point for EU individuals.

4.1.3.3 *Judicial redress*

4.1.3.3.1 Quasi complaint mechanism

204. The so-called "quasi-complaint" procedure allows to act against compulsory collection of information based on a warrant to have an illegal seizure rescinded or altered.

205. This avenue implies the individual is aware of the data being seized. However, the EDPB understands that the procedure for the collection of data based on a warrant is not notified to the data subject. Equally, it understands that voluntary disclosure does not imply that companies requested have the obligation to inform the data subjects of requests received and complied with. Therefore, although it is stressed in the Annex II that "such a challenge can be brought without the individual having to wait for the conclusion of the case", in practice, apart for warrants authorising wiretapping, for which it is indicated that the Law provides for a notification requirement[80], this avenue seems to be effectively available only once the data subject got aware of the collection through a case brought against her or him.

4.1.3.3.2 Injunctive relief

206. In addition, in order to obtain the deletion of data collected through a criminal procedure (the so-called "injunctive relief"), or to obtain compensation of damages, individuals can also bring civil actions before a judge.

207. As regards compensation, the EDPB notes that the procedure seems to be circumscribed to situations where a public officer in the course of his duties, unlawfully and with fault (intentionally or negligently) inflicted damage on the individual concerned. In the understanding of the EDPB, the damage appears to include moral damages. It is however not set out in further detail what needs to be demonstrated by the individual that he/she suffered a damage. The EDPB was not in a position to assess the case law concerning the award of compensation, and is therefore unable to assess whether this avenue provides for an effective remedy in case of damage.

208. With regards to the "injunctive relief", the EDPB also notes that to file a request, the individual should first be aware that his/her data were collected and that they are still retained. Therefore, given the limited rights of information and access of individuals in the context of criminal investigations and procedures, the efficiency of the procedure appears to be rather limited too.

4.1.3.4 *Overall assessment of the avenues for redress*

209. Following the assessment of all the redress avenues open for individuals under Japanese law as well as to the EU data subjects before the PPC, the EDPB welcomes the *ad hoc* dispute resolution mechanism, involving the PPC. It has an added value for EU data subjects, in particular since it allows them to understand which avenues are available for them to obtain redress and/or compensation, as well as to present their requests according to the applicable procedural requirements under Japanese law. However, further clarifications are necessary, in particular on whether and how the mechanism extends the obligations of competent authorities, how they are bound by it, and how the PPC can effectively ensure compliance, in order to ensure that this new mechanism provides for effective redress.

210. This assessment shows that no redress mechanism in Japanese law appears to allow for access, rectification or deletion of data for data subjects who are not victims, suspects or accused in the context of a criminal procedure, for instance to remedy unlawful collection or retention of their data.

[80] Article 23 of the Wiretapping Act is mentioned page 33 of the draft adequacy decision, however the EDPB was not provided with this text and is therefore unable to assess to which extent this notification obligation applies and in which cases it might be limited.

It also shows that all redress and compensation mechanisms and procedures available under Japanese law for victims, suspects or accused person imply the knowledge of the collection of data, which appears to be limited in practice since limited rights of access and information are provided for them. In addition, further clarification appears necessary about the demonstration of an illegal behaviour on the part of the authorities, in particular whether such behaviour includes any illegal processing of personal data, or of a damage suffered by the individual.

211. Therefore, without further documentation and elements, the EDPB is concerned as to whether redress under Japanese law and under the draft adequacy decision is sufficiently effective compared to the standards in EU law.

4.2 Access for national security purposes

4.2.1 Scope of surveillance

212. In the draft adequacy decision, the chapter on "access and use by Japanese public authorities for national security purposes" is introduced by a general statement, in line with the reassurance provided by the Japanese government in Annex II, according to which no Japanese law would provide and thus permit "compulsory requests for information or "administrative wiretapping" outside criminal investigations". As a conclusion, it is said that "on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure. This excludes any covert surveillance activities in this area. Business operators receiving a request for voluntary cooperation (in the form of disclosure of electronic information) are under no legal obligation to provide such information."[81]

213. Within these limitations, four government entities are listed which have the power to collect electronic information held by Japanese business operators on national security grounds. With regard to the Ministry of Defence, as one of those four entities, it is said that it "only has authority to collect (electronic) information through voluntary disclosures".[82]

214. For its assessment of the general setup of data collection for the purpose of national security, the EDPB wishes to recall the first of the four so called "essential guarantees", according to which "processing should be based on clear, precise and accessible rules".[83] More specifically, the ECHR has been very clear that surveillance programs are only "in accordance with the law" if the surveillance measures "have some basis in domestic law". The court has clarified that compatibility with the rule of law requires the law authorizing the measure must be accessible and foreseeable as to its effects. Referring to the risk of arbitrariness, the court has required "clear, detailed rules on secret surveillance measures"; "sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure".[84]

215. For the application of these essential guarantees to the legal system of Japan, the EDPB is aware not only of the fact that, in matters of national security, states have a broad margin of appreciation, recognized by the European Court of Human Rights. Also, national security powers reflect the historical experiences nations make. The EDPB thus understands that, as emphasized by the Japanese

[81] Adequacy decision, paragraph 151.
[82] Adequacy decision, paragraph 153.
[83] WP29, WP 237: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).
[84] See e.g. Big Brother Watch and others v. the United Kingdom, paragraph 305.

government, after World War II, Japanese national intelligence agencies have been equipped with more limited powers than in other states.

216. In the reading of the EDPB, the draft adequacy decision, in line with the reassurance by the Japanese government, suggests that Japanese government entities do not run programs, which strategically monitor or broadly surveille (internet) communication. As said above, the Japanese government has given reassurance, in a letter signed by the Minister of Justice, that "on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure".

217. As to the legal basis of the Ministry of Defence, the EDPB notes that the draft adequacy decision includes general information about its powers and quotes its mission "to conduct such affairs as related thereto in order to secure national peace and independence, and the safety of the nation". However, the EDPB has not been provided with an English translation of the legal basis.

218. At the same time, the EDPB is aware of reports published in different media suggesting that surveillance programs are run by the Directorate for Signals Intelligence of Japan's Ministry of Defense (MOD).[85] In the report, it is also claimed that the Japanese Ministry of Defense, while refusing to discuss specifics of the report, has "acknowledged that Japan has "offices throughout the country" that are intercepting communications" and that those "would be focused on military activities and "cyberthreats" and are "not collecting the general public's information". The latter statement (that the MOD does not collect information on the general public) is made part of the restatement by the Japanese government.

219. It stands that the Japanese government has restated, in a letter signed by the Minister of Justice, that the MOD does not collect information on the general public.

220. It is beyond the task of the EDPB to make a general assessment of the possible surveillance capabilities of the Japanese government. Those activities are only important for its assessment if they are relevant for the transfer of personal data between the EU and Japan. In this context, the EDPB would like to reaffirm its approach already adopted by its predecessor when asked to opine on the EU-U.S. Privacy Shield. When giving an opinion on the Privacy Shield, the WP29 included in its analysis the powers and limits of the U.S. to conduct surveillance of data "on its way" to the U.S.[86] Applying the same standard for the adequacy decision on Japan, the EDPB takes the view that information on the powers of Japanese authorities to surveille data "on its way" to Japan are relevant. Should these surveillance powers exist, also the decision in Big Brother Watch by the ECHR appears to suggest that such powers would have to be regulated in accordance with the standards established by the ECHR.

221. As a consequence, if interceptions were limited to the "assistance of military action", they may well not be relevant for the assessment of the adequacy decision. It is thus the interest of the EDPB to receive clarifications on the surveillance measures by Japanese governmental entities. In this respect, such clarification would be welcome in order to determine whether data undergoing transfer under

[85] In May 2018, the online news publication "The Intercept" published a report titled "The untold story of Japan's secret spy agency".

[86] See WP255, EU-U.S. Privacy Shield –First annual joint review, adopted on 28 November 2017, p. 16: "WP29 is of the view that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third-country's law which enable it to conduct surveillance outside its territory as far as EU data are concerned. As already underlined in its previous opinion, "it should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place, which means including as regards data "on its way" to that country."

this adequacy framework could be the subject of access for national security purposes by the Japanese competent authorities in that field.

4.2.2 Voluntary disclosure in case of national security

222. The draft adequacy decision states that the four government entities only have the authority to collect (electronic) information by voluntary disclosure. According to the draft decision and Annex II, there are some limitations on statutory grounds, which means that the collection of data is limited to what is necessary for the execution of the tasks by the entities.

223. In the area of criminal law, as mentioned in the section about law enforcement, voluntary disclosure is only permissible as part of a criminal investigation, and thus presupposes a concrete suspicion of a crime that is already committed. Investigations in the area of national security differ from investigations in the area of law enforcement. The EDPB acknowledges that, according to Annex II, the central principles of "necessity for investigation" and "appropriateness of method" similarly apply in the area of national security and have to be complied with taking appropriate account of the specific circumstances of each case.[87] It regrets that the application is not further clarified, including by way of further reference to case law. Nevertheless the EDPB states, that the use of this procedure has to be proportionate or necessary.

224. According to the draft decision, when personal information has been collected ('obtained'), its handling is governed by the APPIHAO except for the Prefectural Police.[88] Annex II states that the handling of personal information by the Prefectural Police is governed by prefectural ordinances that stipulate principles for the protection of personal information, rights and obligations equivalent to the APPIHAO.[89] Because there are no English translations available for these ordinances, the EDPB is not in a position to assess whether the principles are equivalent to those of the APPIHAO.

225. For the other remarks on voluntary disclosure, reference is made to the section on law enforcement.

4.2.3 Oversight

4.2.3.1 General Points

226. The four government entities empowered to collect electronic information held by Japanese business operators on national security grounds, are: (i) the Cabinet Intelligence & Research Office (CIRO); (ii) the Ministry of Defence ("MOD"); (iii) the police (both National Police Agency (NPA)[90] and Prefectural Police); and (iv) the Public Security Intelligence Agency ("PSIA").

227. According to the draft adequacy decision, these government entities are subject to several layers of oversight from three branches of the government[91]. The EDPB notes that there are oversight mechanism within the legislative branch (Japanese Diet) and the executive branch (Inspector General's Office of Legal Compliance (IGO), the Prefectural Public Safety Commissions and the Public Security Examination Commission). The EDPB stresses that the COM should clarify the judicial oversight *(ex-officio*/guarantee C of the WP 237; for redress, there is a separate chapter in the draft decision and an extra guarantee in the WP 237) of the above-mentioned government bodies, as it is unclear whether

[87] See Annex II, pp. 23.
[88] Adequacy decision, paragraph 118 and 157.
[89] See Annex II, pp. 3.
[90] However, according to the information received, the main role of the NPA is to coordinate investigations by the various Prefectural Police departments and its information collection activities are limited to exchanges with foreign authorities.
[91] See Annex II, pp. 39.

there is such a judicial oversight in the area of collection of personal information for national security purposes without compulsory means.

4.2.3.2 Oversight by the Japanese Diet

228. The EDPB notes that the Japanese Diet may conduct investigations in relation to the activities of public authorities, therefore also for all of the aforementioned government entities. Furthermore, the diet may also request the production of documents and the testimony of witnesses (*Article 62 of the Japanese Constitution, Article 104 Diet Law*). The EDPB also remarks that according to *Articles 74 and 75 Diet Law*, Diet members may ask written questions to the Cabinet which may end in an answer from the Cabinet (*Article 75 Diet Law*). Finally, it is as well noted that there are specific reporting obligations for e.g. the Public Security Intelligence Agency (PSIA) (Article 36 SAPA/Art 31 ACO), by means of a yearly report to the Diet. Such a report was not provided to the EDPB.

4.2.3.3 Oversight by the Inspector General's Office of Legal Compliance (IGO)

229. The EDPB notes that there is an oversight body for the MOD, called IGO. The EDPB was not provided with the MOD Establishment Act (Act for the Establishment of the MOD), but only with the representations in Annex II to the draft decision. Pursuant to Annex II, the IGO is an independent office within the MOD, which is under the direct supervision of the Minister of Defense according to Article 29 of the MOD Establishment Act. The IGO has the powers of carrying out inspections of compliance with laws and regulations by officials of the MOD (« so called « Defense Inspections »), across the entire ministry including the Self-Defense Forces.

230. Pursuant to the Annex II, the IGO performs its duties independently from MOD's operational departments. The EDPB notes that the IGO is an *internal* oversight body.

231. Inspections lead to findings and, with the intention to ensure compliance, measures which are directly reported to the Minister of Defence. Based on the report of the IGO, the Minister of Defence may issue orders to implement the measures necessary to remedy the situation. The Deputy Vice minister of Defence is responsible for implementing these measures and must report to the Minister of Defence on the status of such an implementation.

232. Analysing Annex II, without being provided with the legal provisions (MOD Establishment Act) for this considerations, the EDPB welcomes the possibility of ordering necessary compliance measures to remedy the situation. However, the EDPB raises doubts regarding the independence of the IGO, as it is an office within the MOD and is under direct supervision of the Minister of Defence pursuant to Annex II (according to the *WP 237* « *functional independence is not by itself sufficient to protect that supervisory authority from all external influence*»).

233. In alignment to the case law of the ECHR and the *WP 237* respectively following the considerations of Annex II, the Inspector General can request for reports from the concerned office (documents, sites, explanations). Clarification as to whether the offices concerned are obliged to follow these requests or not and whether the requested documents include closed materials, like the *WP 237* mentions or not, appear necessary to the EDPB.

234. Although the EDPB welcomes that very senior legal experts (former Superintending Prosecutor) head the IGO, clarification about the manner of appointment of this supervisory body appears necessary.

4.2.3.4 Oversight by Public Security Examination Commission

235. According to Annex II (page 25), PSIA carries out regular and special inspections on the operations of its individual bureaus and offices (Public Security Intelligence Bureau, Public Security Intelligence Offices and Sub Offices, etc). For the purposes of the regular inspection, an Assistant Director General

and/or a Director are designated as inspectors. Such inspections should also concern the management of personal information.

236. Pursuant to recital 163 of the draft decision the *Public Security Examination* Commission operates as an independent ex ante oversight body for the PSIA, with regards to issues of the ACO[92] and SAPA[93]. The EDPB welcomes that.

237. Although the website of the Japanese Ministry of Justice provides some information[94], the EDPB is not in the position to carefully further assess the independency of the Public Security Examination Commission since it was not provided with the Act of the establishment of the Public Security Examination Commission[95] and the Rules of the Public Security Examination Commission[96].

4.2.3.5 Oversight by National Public Safety Commission, Prefectural Public Safety Commissions and the APPIHAO (executive)

238. See 3.1.2.2.1 (National Public Safety Commission), 3.1.2.2.2. (Prefectural Public Safety Commissions) and 3.1.2.2.4. (Executive).

4.2.3.6 Oversight by PPC

239. The EDPB invites the COM to either mention in Recital 164 that the PPC is not an oversight body for the aforementioned government entities and that it is only competent for the redress of the individuals or to move the passage in recital 164 about the PPC to the section « individual redress ».

4.2.4 Redress mechanism

240. For the analysis of the newly negotiated redress mechanism, reference is made to the section on law enforcement.

241. In addition, it is noteworthy that the Japanese law provides for a specific individual redress avenue available in the area of national security. It is the understanding of the EDPB that all individuals, including EU individuals, may generally request disclosure, correction (including deletion) or suspension of use from the administrative organs, also if those are processed for national security purposes. In case such a request is "rejected on the grounds that the concerned information is considered non-disclosable", an appeal for review may be lodged, and the "Information Disclosure and Personal Information Protection Review Board" has to be consulted. The Board is composed of members appointed by the Prime Minister with the consent of both Houses, equipped with investigative powers, and concludes with a written report for the concerned individual, which is not

---

[92] Act on the Control of Organizations Which Have Committed Acts of Indiscriminate Mass Murder (Act No. 147 of December 7, 1999).
[93] Subversive Activities Prevention Act(Act No. 240 of July 21, 1952).
[94] See http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (September 2018): the extra-ministerial organ "*is composed of a chairperson and six members. They are selected from among persons of good character who are capable of making a fair judgment on the control of organizations and those who have ample knowledge and experience of both law and society. They are appointed by the Prime Minister and must be approved by both houses of the Diet. With regard to the application of the previously mentioned laws (SAPA/ACO), the members perform their duties quite independently, free from any direction or supervision of the Prime Minister or the Minister of Justice.*"
[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (September 2018).
[96] Article 28 ACO.

legally binding, but almost always followed.[97] According to Annex II, there were only two out of 2000 cases, where an administrative authority took a decision that differed from the Board's conclusion.[98]

242. It appears to follow from the explanation provided that the review is not available, if the information can be "disclosed" but the individual is dissatisfied with the outcome. The EDPB acknowledges this avenue for redress, but would like to seek further clarification on the latter aspect, which would significantly limit its scope.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[97] Annex II, p. 25, 26. Act for Establishment of the Information Disclosure and Personal Information Protection Review Board, Art. 4, 9, 11.
[98] Annex II, footnote 35.