South Carolina "Adequacy" with the European Union General Data Protection Regulation

Alexander McD. White

Deputy Chief Privacy Officer

South Carolina Department of Administration, Office of Technology and Information Services, Enterprise Privacy Office

January 2019

Introduction

The mission of the South Carolina Department of Administration (Admin) is: "Lead to identify efficiencies. Collaborate to provide services to enhance security and trust. Innovate to increase effectiveness."[1] To fulfill this mission, Admin's Office of Technology and Information Services (OTIS) "provides strategic direction and guidance for the delivery of technology, security, and privacy-related services and solutions to governmental entities." [2] As a member of OTIS's Enterprise Privacy Office (EPO), the author "advises State agencies on the management of personal information," and works "to establish, assess, and enhance privacy protection policy, training, and compliance measures."[3]

The purpose of this paper is to examine a statewide privacy compliance challenge relating to the European Union's General Data Protection Regulation. The following exploratory analysis represents the opinions of the author, not necessarily those of his agency or office, and is intended to spark a statewide conversation on economic and regulatory opportunities in the field of data protection and the steps needed to realize them.

Problem Statement

On May 25, 2018 the European Union (EU)'s General Data Protection Regulation (GDPR)[4] concerning privacy of personal information entered into effect. Widely considered to be a more stringent regulation than any other jurisdiction's laws, the GDPR both created

---

[1] SC Department of Administration web site. https://admin.sc.gov/. Accessed 8 Jan 2019.
[2] SC Department of Administration web site. https://www.admin.sc.gov/executive-director. Accessed 18 Dec 2018.
[3] SC Department of Administration, Enterprise Privacy Office web site. https://www.admin.sc.gov/technology/enterprise-privacy/about-enterprise-privacy. Accessed 18 Dec 2018.
[4] "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 (General Data Protection Regulation)." http://data.europa.eu/eli/reg/2016/679/oj. Accessed 18 Dec 2018.

compliance obligations for organizations that collect or process personal data and enumerated enforceable rights that individuals may exercise to exert control over the use of information relating to themselves. While a full description of the GDPR's requirements are beyond the scope of this paper, examples of compliance challenges for organizations include:

- Developing the capability to respond to individuals' requests to access, edit, or even, depending on the circumstances, delete personal data;
- Utilizing a prescribed "Data Protection Impact Assessment" to analyze the sensitivity of data or the risk of harm to an individual if the data was used in an inappropriate or unauthorized way; and
- Implementing information security controls proportionate to the sensitivity, including notifying regulators of data breaches within seventy-two hours of becoming aware.

EU lawmakers and regulators consider the GDPR's reach to extend beyond the borders of EU Member States. According to their interpretation, any organization collecting or processing data relating to any of the half-billion EU residents must comply with the GDPR. As one of its requirements, organizations are restricted from transferring personal data outside of the EU, [5] since other countries are presumed not to sufficiently respect, protect, or enforce the privacy rights of individuals.

Due to extensive exchanges in trade, travel, tourism, and residency amongst South Carolina and European citizens, such a restriction could have a dramatic effect on the economic prosperity and effective government operations in the state.[6] Data transfers would still be

[5] GDPR Ibid. Article 44: General principles for transfers.

[6] Note: As with many aspects of the law that have not yet been clarified by regulators, GDPR's direct applicability to US state government entities is debatable. Like any other type of organization, a government entity operating entirely outside the EU is considered to be outside the scope of EU law. However, any organization that targets EU

possible, but would involve each organization undergoing a regulatory review of their procedures[7] or determining an exception that applies to the specific situation.[8]

As another option for data transfers, the EU established a political process in which jurisdictions are evaluated to determine whether their respect for and protection of privacy as a fundamental human right is "Adequate," or equivalent to the EU's.[9] While these adequacy determinations existed under previous regulations, the GDPR explicitly contemplates the possibility that sub-national territories or even industry sectors may be approved.[10]

This paper will examine the components of an adequacy decision and apply the logic to South Carolina's environment to determine the legal or regulatory gap, if any, between South Carolina and jurisdictions deemed adequate as well as what steps may be needed to close any gaps. A statewide adequacy decision would have effects beyond state agency compliance issues: it would allow South Carolina businesses to seamlessly offer goods and services to the European market. An adequacy determination would establish the state as one of the most attractive US bases of operation for European companies and enable South Carolina to promote business opportunities and job growth.

Data Analysis

A dozen countries, including the United States (US) to a limited extent, have been granted an adequacy decision by the European Commission, the executive body of the EU.[11]

---

residents could theoretically trigger GDPR compliance requirements. For more on this topic, see Appendix, "Will GDPR Impact States and Localities?" (www.GovTech.com).

[7] GDPR Ibid. Article 47: Binding corporate rules.

[8] GDPR Ibid. Article 48: Derogations for specific situations.

[9] GDPR Ibid. Article 45: Transfers on the basis of an adequacy decision.

[10] GDPR ibid. Article 45(3).

[11] "The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of

While these decisions were made by gauging the countries' compliance with GDPR's predecessor, the Data Protection Directive,[12] the logic proves illustrative, particularly when examining evaluations of the United States' legal environment. In addition, the Commission has recently engaged with Japan and South Korea to discuss an adequacy decision; the products of these dialogues provide additional insight into critical factors.

Elements for Adequacy

In Article 45(2), GDPR outlines three elements in the test by which the Commission examines potential territories for whether they provide an adequate level of protection. They are:

a) "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization…, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
b) "the existence and effective functioning of one or more independent supervisory authorities in the third country…, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers,

America (limited to the Privacy Shield framework) as providing adequate protection." European Commission web site. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. Accessed 18 Dec 2018.

[12] "Directive 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." http://data.europa.eu/eli/dir/1995/46/oj. Accessed 18 Dec 2018.

for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

c) "the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

EU-US Privacy Shield

Despite historical disagreements over the approach to data protection laws and regulations, due to the importance of the trade relationship between the US and EU the two parties have persisted in finding solutions to allow international data transfers. While there have rarely been concerns about the adequacy of US rule of law, approval of US adequacy has turned on issues of public authorities' access to personal data and the functioning of effective and independent regulatory authorities. For example, after revelations by national security contractor Edward Snowden that the US government engaged in national security data collection practices more broadly than commonly understood, the European Court of Justice invalidated the EU-US Safe Harbor framework, ending the most common legal basis for data transfers.[13]

The US and EU negotiated a replacement, the EU-US Privacy Shield Framework, a set of agreements and promises by the US executive branch that the European Commission subsequently deemed adequate protection of privacy rights.[14] As part of the agreement, the Commission will conduct annual evaluations of US compliance with commitments.

[13] "PRESS RELEASE No 106/15, Court of Justice of the European Union. Advocate General's Opinion in Case C-362/14." https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf. Accessed 19 Dec 2018.

[14] Privacy Shield Framework web site. https://www.privacyshield.gov/welcome. Accessed 19 Dec 2018.

In its second annual review in 2018, Privacy Shield was approved to continue for another cycle.[15] The Commission noted US efforts to resolve concerns relating to national security data collection, including reauthorization of critical sections of the Foreign Intelligence Surveillance Act and introduction of "some limited additional privacy safeguards, for instance in the area of transparency."[16] The Commission also positively cited strong oversight of government activities via the Privacy and Civil Liberties Oversight Board and of the private sector via enforcement "mechanisms to detect potential compliance issues, such as random spot-checks[,]…the monitoring of public reports about the privacy practices of Privacy Shield participants[, and] using a variety of tools" to identify false claims of participation by organizations.[17]

The Commission's main concerns and recommendations[18] for this cycle are that:

- US regulators continue to "proactively monitor compliance," detect false claims, and collaborate with EU authorities on points of clarification.
- The government appoints a permanent and effective Ombudsperson to receive and resolve complaints.
- The US adopt as a legal model a comprehensive regulatory system and join international privacy agreements such as Council of Europe's Convention 108.[19]

[15] See Appendix, "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the second annual review of the functioning of the EU-U.S. Privacy Shield." 19 Dec 2018.
[16] Ibid. Page 4.
[17] Ibid. Pages 2-3.
[18] Ibid. Page 5-6.
[19] Note: The current US regulatory framework consist of "sectoral" laws that apply to certain industries and "self-regulatory" standards voluntarily adopted by industries or individual organizations. An example of a sectoral law would be the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which has a limited scope and applies primarily to healthcare providers. An example of a self-regulatory system is the Payment Card Institute Data Security Standard (PCI DSS), which is a set of rules created by credit card companies and enforced through contract. The EU-US Privacy Shield has elements of a self-regulatory system, in that organizations comply by choice, but the framework has been given the force of law for those who do so choose ("co-regulatory"). In the EU and other countries, "comprehensive" privacy laws broadly apply to any collection or use of personal data

Japan

Throughout 2018, the EU and Japan have engaged in talks to establish mutual recognition of adequacy as part of a larger free trade deal. These discussions, which still await a final decision, are noteworthy in that they involve the first application of GDPR standards for adequacy to a new territory.

As with the Privacy Shield discussions, EU authorities negotiated commitments from the government beyond the standard data protection laws of the country. Since the Japanese privacy regulator enshrined these commitments as "legally binding rules, any rights and obligations are enforceable … in the same way as the provisions of the Act that they supplement with stricter and/or more detailed rules."[20] The rules added, among other matters, specificity regarding special categories of data that are considered more sensitive, organizations' obligations regarding identification and communication of the purpose for data collection, and the circumstances in which it would be permissible to transfer data that relates to EU residents outside of Japan.

As part of the adequacy decision-making process, a group of EU privacy regulators called the European Data Protection Board (EDPB), provides an opinion to guide the Commission. In its Opinion 28/2018,[21] the EDPB cites concerns relating to:

- the patchwork nature of combining the privacy law with Supplementary Rules. The EDPB seeks clarity about the legally binding status of the rules;[22]

---

regardless of industry. For more, see: Swire, Peter P., and Kenesa Ahmad. *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices*. Edited by Terry McQuay, IAPP, 2012. p. 29-45.

[20] See Appendix, "Annex I: 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." Page 2.

[21] See Appendix, "Opinion of the Board (Art. 70.I.s), Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan."

[22] Ibid. Paragraphs 12-13.

- the ability of the Japanese regulator to determine third countries that will be considered adequate from a Japanese perspective, creating the risk of a data funneling from the EU in unanticipated ways;[23]
- consent as a basis for processing in the Japanese legal system and for transfers to third countries, since "the information given to the EU data subject prior to consenting seems not to be comprehensive;"[24]
- the ability of Europeans to access the Japanese legal or redress system due to sole Japanese language availability for regulatory guidance. The EDPB would "welcome … an online service, at least in English";[25] and
- law enforcement and national security redress and oversight mechanisms, as well as the ability of the EDPB to conduct a thorough review of these mechanisms due to the unavailability of translations of legal and court documents.[26]

As of December 2018, the concerns raised by the EDPB and other parties indicate that "further clarifications," or another round of discussions, may be needed before a final decision.[27]

South Korea

South Korea and the EU began adequacy talks in 2015 prior to the creation of the GDPR, but European concerns about effective and independent regulators have prevented approval of the country to date. As cited above, Article 45(2)(b) of the GDPR states that regulatory authorities must have three characteristics. They must be:

---

[23] Ibid. Paragraph 17.
[24] Ibid. Paragraphs 18, 98.
[25] Ibid. Paragraph 29.
[26] Ibid. Paragraph 27 and Section 4.
[27] "Japan's long road for adequacy under the GDPR." https://iapp.org/news/a/japans-long-road-for-adequacy-under-the-gdpr/. Accessed 20 Dec. 2018.

"*independent* supervisory authorities," not a part of the political government, "with *responsibility for ensuring and enforcing compliance* with the data protection rules, including adequate *enforcement powers*…" [emphasis added]

In South Korea "multiple government agencies play supplemental roles" with complementary or overlapping supervisory authority. [28] The Personal Information Protection Commission (PIPC) is an independent authority with supervision over the comprehensive privacy law but without enforcement powers; those powers are actually held by the Ministry of the Interior and Safety (MOIS).[29] There is an entity that arguably meets all three requirements, the Korean Communications Commission (KCC), but its powers are limited to supervising the broadcasting and communications sector. The KCC consists of two commissioners "directly appointed by the President …[and] three are nominated by the National Assembly."[30]

Table 1:

Entity	**Independent?**	**Responsibility?**	**Enforcement Powers?**
PIPC	Yes	Yes, most organizations	No
MOIS	No	Yes, most organizations	Yes
KCC	Yes	Yes, Broadcasting and Communications only	Yes

[28] "Structure and Enforcement of Data Privacy Law in South Korea." Brussels Privacy Hub Working Paper Vol. 2. No. 7. October 2016.
[29] Ministry of the Interior and Safety web site. https://www.privacy.go.kr/eng/about_us.do. Accessed 28 Dec 2018.
[30] Korea Communications Commission web site. https://eng.kcc.go.kr/user.do?page=E01010100&dc=E01010100. Accessed 28 Dec 2018.

While the country considered an adequacy application limited to only the Broadcasting and Communications sector, instead legislators sought to remedy the regulatory gaps in independence and powers.[31] A newly proposed law from November 2018 will combine the enforcement powers of MOIS and KCC and grant them to the PIPC. Commentators state that after such a change, "South Korea will be in a good position to obtain an EU adequacy decision."[32]

South Carolina

The Constitution of South Carolina enshrines privacy as a fundamental right. The Declaration of Rights[33] Article I, Section 10 protects "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy". Article I, Section 2 prohibits the state legislature from, among other matters, "bridging the freedom of speech or of the press; or the right of the people peaceably to assemble and to petition the government or any department thereof for a redress of grievances." In addition, the Declaration of Rights contains protections relating to due process[34] and the rule of law,[35] seizure of private property,[36] judicial review of administrative agencies,[37] and the rights of victims.[38]

---

[31] "South Korea's EU adequacy decision rests on new legislative proposals." https://iapp.org/news/a/south-koreas-eu-adequacy-decision-rests-on-new-legislative-proposals/. Accessed 20 Dec 2018.
[32] "Proposed Changes to South Korea's Personal Information Protection Act." https://www.jdsupra.com/legalnews/proposed-changes-to-south-korea-s-96538/. Accessed 20 Dec 2018.
[33] See Appendix, ARTICLE I DECLARATION OF RIGHTS.
[34] Ibid. Article I, Section 3: Privileges and immunities; due process; equal protection of laws.
[35] Ibid. Article I, Section 9: Courts; speedy remedy.
[36] Ibid. Article I, Section 13: Taking private property; economic development; remedy of blight.
[37] Ibid. Article I, Section 22: Procedure before administrative agencies; judicial review.
[38] Ibid. Article I, Section 24: Victims' Bill of Rights.

In the South Carolina legal environment, organizations including state government entities must comply with US federal regulations, such as sectoral laws related to privacy and credit reporting. In addition, like most US states South Carolina has focused its own privacy regulation on issues surrounding data breaches, a subset of data protection. Through a variety of laws, regulations, and legislative provisos, both private and public sector entities are required to notify regulators and affected individuals in the event of a data beach.[39] State agencies face additional privacy and cybersecurity compliance requirements related to their business practices that are developed by the Department of Administration.[40]

Several agencies play a role in privacy regulation and oversight.[41] While some federal privacy laws delegate powers to state Attorneys General, South Carolina laws empower the Department of Consumer Affairs (DCA) to regulate data breach notification obligations.[42] The Attorney General is an elected position, and DCA is an administrative agency governed by a commission "composed of nine members, one of whom is the [elected] Secretary of State. Of the remaining eight members, the General Assembly elects four other members from outside the legislature and the Governor appoints four members whose appointments are confirmed by the Senate."[43] In addition, the mission of the SC Office of Ombudsman is "to appropriately refer any

[39] SC Code Ann. Sec. 39-1-90 Breach of security of business data; SC Code Ann. Sec. 1-11-490 Breach of security of state agency data; SC Code Ann. Sec. 30-2-10, et seq. Family Privacy Protection Act; SC Code Ann. Sec. 30-2-310 et seq. Personal Identifying Information Privacy Protection; SC Legislature 2018-2019 Appropriations Bill as Ratified by the General Assembly on June 29, 2018, Proviso 117.105 Data Breach Notification. (Note: Proviso numbers may change with each annual budget bill.)

[40] SC Legislature 2018-2019 Appropriations Bill as Ratified by the General Assembly on June 29, 2018, Proviso 93.20 Cyber Security; Proviso 117.112 Information Technology and Information Security Plans. (Note: Proviso numbers may change with each annual budget bill.)

[41] Note: As in other US states, the Department of Insurance regulates the insurance industry. In 2018, the South Carolina Insurance Data Security Act (SC Code Ann. Sec 38-99-10 et seq.) empowered the agency to regulate insurance organizations' cybersecurity and privacy programs. While this paper focuses on a statewide adequacy decision, the insurance industry could provide an interesting case study for a sectoral adequacy evaluation.

[42] Inter alia, SC Code Ann. Sec. 39-1-90(H), (K); Sec. 1-11-490(H), (I); Proviso 117.105(G), (H).

[43] SC Department of Consumer Affairs web site. https://consumer.sc.gov/about-us/commission. Accessed 27 Dec 2018.

question, concern, or request a citizen might have[,]…accurately and efficiently navigating South Carolinians to the proper state agency or resource equipped to handle their needs."[44]

Implementation Plan

To achieve an adequacy determination, South Carolina must address the faults found in other countries' frameworks within the context of GDPR Article 45(2). As state subject matter experts on privacy, the Enterprise Privacy Office stands in prime position to support state agencies, legislators, and other stakeholders to evaluate and prepare an adequacy effort.

Rule of Law

The EU-US Privacy Shield negotiations and evaluations indicate that rule of law is, in large part, not an issue for US jurisdictions. Even examination of national security operations, beyond the legal control of South Carolina legislation and regulation, received a favorable opinion in the second annual Privacy Shield review. EU criticisms on this front focused on the perceived need for a permanent and effective federal Ombudsperson and the lack of a comprehensive regulatory system.

South Carolina should undertake a study to cross-reference the duties of the requested federal Ombudsperson with existing state oversight bodies. This study may find that the combined work of the Office of Ombudsman, Department of Consumer Affairs, and potential other groups already provide the appropriate level of governmental oversight.

South Carolina should investigate the benefits and detriments of implementing a comprehensive privacy regulation. While such regulations are rare in the US, they are not

[44] SC Office of Ombudsman web site. http://ombudsman.sc.gov/. Accessed 27 Dec 2018.

without precedent and occur more frequently in other countries. The California Consumer Privacy Act (CCPA) of 2018,[45] signed into law June 2018, created privacy rights for California residents and compliance obligations for businesses similar to those in the GDPR. In addition, several Canadian provinces[46] and Australian states[47] have passed comprehensive legislation at the state government level. This comprehensive law should consider carefully the definition of what is considered personal data and what elements would be considered sensitive data deserving even greater protection.

If a decision is made to forego a comprehensive law, South Carolina should investigate steps needed to achieve the effect through laws or regulations supplementing existing law. Solutions may include executive orders in lieu of legislative action, or a legislative authorization for regulatory rule-making authority for data privacy issues concerning foreign nationals. However, as the evaluations of Japanese adequacy have shown, these supplementary rules may cause lingering doubt that could delay or prevent a favorable final decision.

EU criticisms of the Japanese framework also raised concerns regarding the onward transfer of data to other jurisdictions. South Carolina may be limited in the extent to which the state may prohibit such transfers within the US. The state should investigate whether doing so would be permitted under the US Constitution's interstate commerce provisions. If a prohibition is not possible, the state should investigate how to achieve the desired consumer protection in the alternative, perhaps by requiring that businesses with EU customers limit data transfers to only

[45] California Assembly Bill No. 375. TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Accessed 27 Dec 2018.
[46] Office of the Privacy Commissioner of Canada web site. "Summary of privacy laws in Canada." https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/. Accessed 27 Dec 2018.
[47] Office of the Australian Information Commissioner web site. "Other privacy jurisdictions." https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions#state-and-territory-privacy. Accessed 27 Dec 2018.

Privacy Shield organizations or that any transfer must nevertheless meet all promises made to the consumer in that (or any other) regard.

As part of any new privacy law, the state should evaluate the use of consent as a method for organizations to collect and use data. Concerns raised by the EDPB in their examination of Japan indicate that consent as a legal process may prove difficult to justify, since individuals must receive comprehensive information on data use and transfer for the consent to be valid. South Carolina should investigate the extent to which consent as a legal basis for data processing may be unwieldy to legislate for and regulate.

Effective and Independent Supervision

As part of any new legislation or regulation developed, South Carolina must examine what steps may be needed to ensure privacy regulation is effective and independent. As the South Korea example illustrates, for adequacy the EU desires that regulatory authorities have independence, responsibility for enforcing compliance, and enforcement powers. South Korea chose to address its issues by consolidating enforcement power, and South Carolina should evaluate whether such a course would prove effective. As part of this evaluation, South Carolina should consider whether either or both of the elected Attorney General or DCA oversight commission are sufficiently independent according to the EU standards and definitions.

Under current data breach legislation, privacy violations are only discovered after the breach is self-reported. Based on EU criticisms of Privacy Shield, to achieve compliance South Carolina should ensure that privacy laws and regulations include oversight that is a proactive monitoring of compliance. South Carolina should also develop mechanisms for domestic regulators to collaborate with EU regulators on enforcement issues.

Since South Carolina government operates in English, concerns about European access to the legal or redress system are lesser than those expressed regarding Japan. Still, South Carolina should consider whether to add to online regulatory guidance any additional European languages that may also be spoken in the state.

Legally binding international agreements

The EU recommends that the US join the Council of Europe's Convention 108, a binding privacy treaty. South Carolina should investigate whether the commitments of Convention 108 match with existing state policies and constitutional protections and whether, if it so chose, the state may participate in an international agreement, including as an observer. In addition, South Carolina should investigate opportunities for state privacy regulators to participate in international associations and collaborative bodies.

Evaluation Method

Perhaps the best gauge of these recommendations' success would be the simple binary of whether South Carolina successfully achieves an adequacy status or not. Short of that, a variety of stakeholders will need to collaborate to translate the recommended assessments into specific steps. Privacy, legal, regulatory, and legislative expert evaluations and opinions can help determine whether these suggestions close the gap between current state and GDPR adequacy.

Importantly, adequacy with GDPR does not necessarily mean being identical to GDPR. Reviews such as the Privacy Shield's show that jurisdictions may take alternative approaches. As the EDPB predecessor group stated:

> "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]'. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.'"[48]

Even without an adequacy determination, South Carolina could realize and measure the benefits of proactive and comprehensive privacy regulation through increased European business interactions and improved economic well-being for state residents.

Summary and Recommendations

To summarize, this report recommends the following steps:

- Identify plan of action and timelines for an internal South Carolina evaluation of adequacy actions, with the Enterprise Privacy Office supporting stakeholders as subject-matter experts;
- Analyze the position of Privacy Shield Ombudsperson to ensure that South Carolina government oversight is comparable (include Office of Ombudsman, Department of Consumer Affairs, etc.);
- Investigate comprehensive privacy regulation, using lessons learned from the California Consumer Privacy Act of 2018, and alternatives such as supplementary rules for regulators;
- Investigate to what extent South Carolina may prohibit onward transfers and what alternative actions would meet the spirit of the prohibition;
- Evaluate the use of consent as a justification for organizations to collect and use data, and develop an alternative legal framework for data management;

[48] See Appendix, Article 29 Working Party Adequacy Referential 18/EN WP 254 rev.01. Chapter 1, paragraph 2.

- Examine potential actions to consolidate enforcement power, and develop a position statement on the independence of state regulators;
- Develop mechanisms for domestic regulators to collaborate with EU regulators on enforcement issues;
- Study impact of adding additional European languages to online regulatory guidance;
- Investigate and develop a policy regarding international participation in or observation of privacy treaties and regulatory groups; and
- Develop an engagement strategy on how best to begin adequacy discussions with European Union leadership. The adequacy negotiations may be a time-consuming process, all the more so since South Carolina's would be a trail-blazing sub-national application.

Naturally, once any or all of these recommended actions have been taken, the state should examine the results and necessary follow-up steps to determine if the suggested courses of actions matches other state priorities.

Changing government regulation and regulatory strategy may require more than checklists, but a change in societal attitudes towards data rights. To use an analogy: privacy programs are centered around building trust between an organization and the individual sharing his or her data. Similarly, a GDPR adequacy decision relies as much on trust as on black-letter law. For an application to succeed, the legal privacy protections in the applicant's jurisdiction should reflect the concerted will of the people and show the good faith of both parties to respect and protect privacy as a fundamental right of all individuals.

Appendix

- General Data Protection Regulation, "CHAPTER V, TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS, Articles 44-50."
- "Will GDPR Impact States and Localities?";
- "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the second annual review of the functioning of the EU-U.S. Privacy Shield";
- "Annex I: 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.";
- "Opinion of the Board (Art. 70.I.s), Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan";
- South Carolina Constitution, "Article I, Declaration of Rights"; and
- "Article 29 Working Party Adequacy Referential 18/EN WP 254 rev.01"

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

   On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

   (a) a legally binding and enforceable instrument between public authorities or bodies;

   (b) binding corporate rules in accordance with Article 47;

   (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

   (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

   (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

   (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Articles 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph and the second subparagraph of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

(/)

DATA
(/data)

Will GDPR Rules Impact States and Localities?

The European Union's General Data Protection Regulation (GDPR) May 25 enforcement deadline is fast approaching, but state and local governments shouldn't worry, say experts.

BY DAWN KAWAMOTO (HTTP://WWW.GOVTECH.COM/AUTHORS/DAWN-KAWAMOTO.HTML) / MAY 3, 2018

SHUTTERSTOCK

(http://www.govtech.com/data/Will-GDPR-Rules-Impact-States-and-Localities.pdf)

When the May 25 enforcement deadline for Europe's General Data Protection Regulation (GDPR) (https://ec.europa.eu/info/law/law-topic/data-protection_en) rolls around, U.S. companies, organizations and institutions that target their products and services to people living in Europe will be on the hook to comply or potentially face steep fines.

GDPR is a set of strict rules that give European Union (EU) citizens control over their personally identifiable information (PII).

The rules have instilled fear in a number of these entities, which may face fines of up to 4 percent of their annual global revenue or 20 million euros, whichever is greater, should they fail GDPR compliance. But what about state and local governments?

REGULATORS EXPLAIN GDPR'S IMPACT ON GOVERNMENT

“If a third country processor like a U.S. government agency is not targeting the European market with goods and services, then they would not have to abide by GDPR,” said Dirk Hensel, a spokesman for Germany’s federal commissioner for Data Protection and Freedom of Information. “I don’t think we’ll see too many of these cases are relevant.”

For example, a resident in Germany may own property in Los Angeles County and pay the fee to access their records online through the county’s website. In this particular case, Los Angeles County is not “targeting” Germany’s residents or other European citizens to use the service. It just happens to have a website that can be accessed by German citizens and others throughout the globe, he noted.

However, if the state of Florida’s tourism department, for example, launches a promotional campaign to target residents living in Europe to come visit the Sunshine State, then any PII data collected on those German citizens by the state of Florida would likely fall under GDPR requirements, he explained.

One point Hensel noted, however, is if the Florida tourism department relied on an advertising agency to run its promotional campaign and interact with Germany’s citizens, then it is the advertising agency that needs to abide by GDPR.

Anya Burgess, a spokeswoman with the United Kingdom’s Information Commissioner’s Office, told *Government Technology* that GDPR only applies if individuals who receive the product or service reside in Europe.

As a result, GDPR does not apply if a U.S. government agency collects PII data on a citizen of Europe who is visiting or living in the U.S. and uses that government agency’s services or products while in the U.S.

"If the processing is not going on in the EU to citizens in the EU, then it doesn't apply," Burgess said, noting, "U.S. government agencies provide their services in the U.S. and not the EU and would not be regulated by the GDPR."

State and local government agencies are encouraged to contact EU data authorities (http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm) if they have GDPR questions, Hensel advised.

GDPR DEFINED

Under GDPR, all companies, institutions, organizations and government agencies that process PII on individuals residing in the European Union must abide by these privacy regulations, regardless of where the entity is located.

Overall, the goal of GDPR is to provide European residents with transparency of how their PII data is used, improve the level of control over their own data and increase the safeguards used to protect that data.

GDPR requires entities to request PII data in clear, simple language and attach the consent form to the information on why the data is needed. And before a government agency or other entities can use the PII data, users would need to opt in with their consent and be able to withdraw that consent just as easily, according to the GDPR.

HOLDING EU CITIZEN DATA NOT AN OPTION

Although the impact on state and local governments is expected to be minimal, government agencies are still taking stock of where they potentially stand when it comes to complying with GDPR and safeguarding PII data of EU citizens.

The Washington state Office of Privacy and Data Protection (OPDP) held a staff meeting in March to discuss GDPR issues, according to Will Saunders, senior program manager for open data at Washington's OPDP.

Alex Alben, Washington state chief privacy officer, led the discussion on how much risk Washington state faces under GDPR and one of the issues considered, for example, is the number of Europeans who receive services from the state and what potential risks that could mean to Washington state, Saunders recalled.

"The number of Europeans receiving state services is pretty minimal and the state is already taking efforts to keep its PII to a minimum," said Saunders.

GDPR consultant Sheila FitzPatrick, founder of FitzPatrick & Associates, said state and local governments will not likely have a lot of PII data on European residents, compared to federal agencies.

"Governments tend to hold onto data, but under GDPR, in most circumstances, they won't be able to do that," she warned. "Federal, state and local governments are not exempt under GDPR."

Dawn Kawamoto (http://www.govtech.com/authors/Dawn-Kawamoto.html) Former Staff Writer

Dawn Kawamoto is a former staff writer for *Government Technology*.

RELATED

New European Rules May Give US Internet Users True Privacy Choices for the First Time (http://www.govtech.com/pcio/articles/New-European-Rules-May-Give-US-Internet-Users-True-Privacy-Choices-for-the-First-Time.html)

European GDPR Laws to Take Effect Friday (http://www.govtech.com/policy/America-to-Be-Hit-by-Europes-Data-Law-on-Friday-.html)

Tech Companies Embrace Some GDPR Privacy Practices Outside of Europe (http://www.govtech.com/policy/Tech-Companies-Embrace-Some-GDPR-Privacy-Practices-Outside-of-Europe.html)

DISCUSS

MORE FROM DATA (HTTP://WWW.GOVTECH.COM/DATA)

EUROPEAN
COMMISSION

Brussels, 19.12.2018
COM(2018) 860 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the second annual review of the functioning of the EU-U.S. Privacy Shield

{SWD(2018) 497 final}

1. THE SECOND ANNUAL REVIEW – PURPOSE, PREPARATION AND PROCESS

On 12 July 2016, the Commission adopted a Decision (the "adequacy decision") in which it found that the EU-U.S. Privacy Shield (the "Privacy Shield") ensures an adequate level of protection for personal data that has been transferred from the EU to organisations in the U.S.[1] The adequacy decision notably provides for an annual evaluation of all aspects of the functioning of the framework by the Commission. The first annual review took place on 18 and 19 September 2017 in Washington, D.C., and on 18 October 2017 the Commission adopted its report to the European Parliament and the Council,[2] accompanied by a Commission Staff Working Document (SWD(2017)344 final).[3]

On the basis of its findings from the first review, the Commission concluded that the U.S. continued to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the U.S. At the same time, the Commission considered that the practical implementation of the Privacy Shield framework could be further improved in order to ensure that the guarantees and safeguards provided therein continued to function as intended. To this end, the Commission made ten recommendations.

The present report concludes the second annual review of the functioning of the Privacy Shield. This report, as well as the accompanying Staff Working Document (SWD(2018) 497), follow the same structure as the report on the first annual review. They cover all aspects of the functioning of the Privacy Shield, also in light of developments that took place during the last year. A central element of the Commission's assessment was the implementation of its recommendations from the first annual review.

In preparation for the second annual review, the Commission gathered information from relevant stakeholders (in particular Privacy Shield-certified companies, through their respective trade associations, and non-governmental organisations (NGOs) active in the field of fundamental rights, in particular digital rights and privacy), as well as from the relevant U.S. authorities involved in the implementation of the framework.

The second annual review meeting took place in Brussels on 18 and 19 October 2018. The review was opened by the Commissioner for Justice, Consumers and Gender Equality Věra Jourová, U.S. Secretary of Commerce Wilbur Ross, the Chairman of the Federal Trade Commission Joseph Simons and the Chair of the European Data Protection Board Andrea Jelinek. It was conducted for the EU by representatives of the European Commission's Directorate General for Justice and Consumers. The EU delegation also included seven

[1] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 2017, 1.8.2016, p. 1

[2] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield (COM(2017611 final, see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

[3] Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield (SWD(2017)344 final), see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

representatives designated by the European Data Protection Board (the independent body bringing together representatives of the national data protection authorities of the EU Member States and the European Data Protection Supervisor).

On the U.S. side, representatives from the Department of Commerce, the Department of State, the Federal Trade Commission , the Department of Transportation, the Office of the Director of National Intelligence, the Department of Justice and members of the Privacy and Civil Liberties Oversight Board participated in the review, as well as the acting Ombudsperson and the Inspector General for the Intelligence Community. In addition, representatives from an organisation that offers independent dispute resolution services under the Privacy Shield and the American Arbitration Association provided information during the relevant review sessions. Finally, the review was informed by presentations from Privacy Shield-certified organisations on how companies comply with the requirements of the framework.

The Commission's findings have further been informed by a study commissioned by the Commission and publicly available material, such as court decisions, implementing rules and procedures of relevant U.S. authorities, reports and studies from non-governmental organisations, transparency reports issued by Privacy Shield-certified companies, annual reports from independent recourse mechanisms, as well as media reports.

This year's review took place in the context of the challenges to data privacy that are increasingly global in nature, as exemplified by the Facebook / Cambridge Analytica case. Both the EU and the U.S. are aware of the similar challenges they face when it comes to protection of personal data. During the review, both sides stressed the need to address such abuses of personal data, including through the vigorous enforcement actions by the EU's Data Protection Authority and the U.S. Federal Trade Commission.

The Commission's report also reflects the ongoing debate about federal privacy legislation in the U.S. The convergence between our two systems in the long term would strengthen the foundations on which the Privacy Shield framework has been developed.

2. FINDINGS AND CONCLUSION

The second annual review covered both the "commercial aspects" of the Privacy Shield framework and issues relating to government access to personal data.

As regards the "commercial aspects", i.e. questions concerning the administration, oversight and enforcement of the obligations applying to certified companies, the Commission noted that in line with the Commission's recommendations from the first annual review, the Department of Commerce has further strengthened the certification process and introduced new oversight procedures. In particular, the Department of Commerce adopted a new process that requires first-time applicants to delay public representations regarding their Privacy Shield participation until their certification review is finalised by the Department of Commerce. Moreover, the Department of Commerce has introduced new mechanisms to

detect potential compliance issues, such as random spot-checks (at the time of the annual review, such spot checks had been performed on about 100 organisations) and the monitoring of public reports about the privacy practices of Privacy Shield participants. In the search for false claims of participation in the framework, the Department of Commerce is now actively using a variety of tools, for instance a quarterly review of companies that have been identified as more likely to make false claims and a system for image and text searches on the internet. As a result of these newly introduced practices and procedures, the Department of Commerce since the first annual review has referred more than 50 cases to the Federal Trade Commission, which in turn took enforcement action in those cases where the referral as such was not sufficient in order to make the company concerned come into compliance.

With respect to enforcement, the Commission noted that the Federal Trade Commission, as part of its efforts to proactively monitor compliance with the Privacy Shield Principles, recently issued administrative subpoenas to request information from a number of Privacy Shield participants. The Federal Trade Commission has also confirmed that its investigation into the Facebook / Cambridge Analytica case is ongoing. Although the Commission considers that the Federal Trade Commission's new, more proactive approach to compliance monitoring is an important development, it regrets that at this stage it was not possible for to provide further information on its recent investigations and will closely monitor any further developments in this regard.

The second annual review also took into account relevant developments in the U.S. legal system in the area of privacy. These concern, in particular, the consultation initiated by the Department of Commerce on a federal approach to data privacy as well as the Federal Trade Commission's process of reflection on its current powers in the area of privacy and the efficacy of the use of its current remedial authority.

As the Facebook/Cambridge Analytica case and other revelations have shown, it would be important that the EU and the U.S. further converge in their responses. In this spirit, the Commission has observed the abovementioned initiatives with great interest and has contributed to the Department of Commerce's consultation process with a written submission[4].

Regarding aspects relating to access and use of personal data by U.S. public authorities, the second annual review focused on relevant developments in the U.S. legal framework, including with regard to relevant agency policies and procedures, on recent trends in surveillance activities, and on developments in the setup and functioning of important oversight and redress mechanisms.

The most important legal development in the area of government access was the reauthorisation of Section 702 of the Foreign Intelligence Surveillance Act ("the Act") at the beginning of 2018. While the reauthorisation did not lead to the incorporation of the protections of Presidential Policy Directive 28 into the Act, as had been suggested by the

[4] Available at https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf

Commission, neither did it restrict any of the safeguards contained in the Act which were in place when the Privacy Shield decision was adopted. Moreover, the amendments did not expand the powers of the U.S. Intelligence Community to acquire foreign intelligence information by targeting non-U.S. persons under Section 702. Instead, the Amendments Reauthorization Act of 2017, which amends the Foreign Intelligence Surveillance Act of 1978, introduced some limited additional privacy safeguards, for instance in the area of transparency.

There have also been important developments concerning the Privacy and Civil Liberties Oversight Board which, at the time of the first annual review, had only one Board member left. The Commission had therefore recommended the swift appointment of the missing Board members. On 11 October 2018, the U.S. Senate confirmed the nominations of the Chairman of the Privacy and Civil Liberties Oversight Board as well as of two other members of the Board, thereby reinstalling the Board to its full quorum and allowing it to exercise all its functions. After the first annual review, the Commission had also recommended the public release of the Board's report on Presidential Policy Directive 28. The report was released on 16 October 2018[5] and confirms that Presidential Policy Directive 28 is fully applied across the Intelligence Community. In particular, it confirms that further to the issuance of Presidential Policy Directive 28, the relevant elements of the Intelligence Community have adopted detailed rules on the implementation of that Directive and have changed their practices in order to bring them in line with the requirements of Presidential Policy Directive 28.

Finally, although the Commission had recommended the swift appointment of the Privacy Shield Ombudsperson, the position of Under-Secretary in the State Department to whom the office of the Ombudsperson has been assigned had not yet been filled by a permanent appointment at the time of the present report. In that regard, the Commission took note of the fact that at the second annual review, the U.S. government recognised the need for prompt progress on nominating a permanent Under Secretary and confirmed that this process is well underway.

At the time of the present report, the Ombudsperson mechanism had not yet received any requests. However, a complaint to the Ombudsperson had been submitted to the Croatian data protection authority and the relevant checks were ongoing.

The detailed findings concerning the functioning of all aspects of the Privacy Shield framework after its second year of operation are presented in the Commission Staff Working Document on the second annual review of the functioning of the EU-U.S. Privacy Shield (SWD(2018) 497) which accompanies the present report.

The information gathered in the context of the second annual review confirms the Commission's findings in the adequacy decision, both with regard to the "commercial aspects" of the framework and aspects relating to access to personal data transferred under the Privacy Shield by the U.S. authorities.

[5] Report to the President on "the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities", available at https://www.pclob.gov/reports/report-PPD28/

On the basis of these findings, the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shieldfrom the Union to organisations in the United States.

In particular, the steps taken to implement the Commission's recommendations following the first annual review have improved several aspects of the practical functioning of the framework in order to ensure that the level of protection of natural persons guaranteed by the adequacy decision is not undermined.

However, some of these steps have been taken only recently and the relevant processes are still ongoing. Any further developments concerning these processes therefore need to be closely monitored, in particular as they affect elements that are essential for the continuity of the adequacy finding. This concerns notably:

1. The effectiveness of the mechanisms introduced by the Department of Commerce in the second year of operation of the framework to proactively monitor compliance by certified companies with the Privacy Shield Principles, in particular compliance with substantive requirements and obligations.

2. The effectiveness of the tools introduced by the Department of Commerce since the first annual review to detect false claims of participation in the framework, with a particular focus on the search of false claims by companies that have never applied for certification.

3. The progress and outcome of ex-officio sweeps carried out by the Federal Trade Commission in the second year of operation of the Privacy Shield by means of administrative subpoenas to detect substantive violations of the Privacy Shield.

4. The development of additional guidance jointly by the Department of Commerce, Federal Trade Commission and EU data protection authorities on elements that require further clarification (e.g. HR data).

5. The appointment of a permanent Privacy Shield Ombudsperson.

6. The effectiveness of the handling and resolution of complaints by the Ombudsperson.

In particular, the Commission reiterates its call on the U.S. administration to confirm its political commitment to the Ombudsperson mechanism by appointing a permanent Privacy Shield Ombudsperson as a matter of priority. The Ombudsperson mechanism is an important element of the Privacy Shield framework and, while the acting Ombudsperson continues to carry out the relevant functions, the absence of a permanent appointee is highly unsatisfactory and should be remedied as soon as possible. The Commission expects the U.S. government to identify a nominee to fill the Ombudsperson position on a permanent basis by 28 February 2019 and inform the Commission about the nominated individual. If this does not take place

by that date, the Commission will then consider taking appropriate measures, in accordance with the General Data Protection Regulation[6]. The Commission also expects to receive precise and detailed information on all of the abovementioned aspects in order to be able to assess whether the steps taken are effective in practice.

Finally, the Commission will continue to closely follow the ongoing debate about the federal privacy legislation in the U.S. Given the significance of transatlantic data flows, the Commission encourages the U.S. to adopt a comprehensive system of privacy and data protection and to become a Party to the Council of Europe's Convention 108. It is through such comprehensive approach that convergence between our two systems can be achieved in the longer term, which would also strengthen the foundations on which the Privacy Shield framework has been developed.

[6] 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 (General Data Protection Regulation)

Annex I

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

Table of Contents

[Terms]

“Act”	The Act on the Protection of Personal Information (Act No. 57, 2003)
“Cabinet Order”	Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order No. 507, 2003)
“Rules”	Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 3, 2016)
"General Rules Guidelines"	Guidelines for the Act on the Protection of Personal Information (Volume on General Rules) (Notice of the Personal Information Protection Commission No. 65, 2015)

“EU”	European Union, including its Member States and, in the light of the EEA Agreement, Iceland, Liechtenstein and Norway
“GDPR”	Regulation of the European Parliament and of the Council 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（General Data Protection Regulation）
“adequacy decision”	The European Commission’s decision that a third country or a territory within that third country, etc. ensures an adequate level of protection of personal data pursuant to Article 45 of the GDPR

The Personal Information Protection Commission, for the purpose of conducting mutual and smooth transfer of personal data between Japan and the EU, designated the EU as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests based on Article 24 of the Act and the European Commission concurrently decided that Japan ensures an adequate level of protection of personal data pursuant to Article 45 of the GDPR.

Hereby, mutual and smooth transfer of personal data will be conducted between Japan and the EU in a way that ensures a high level of protection of an individual's rights and interests. In order to ensure that high level of protection regarding personal information received from the EU based on an adequacy decision and in light of the fact that, despite a high degree of convergence between the two systems, there are some relevant differences, the Personal Information Protection Commission has adopted these Supplementary Rules, based on the provisions of the Act concerning implementation etc. of cooperation with the governments in other countries and in view of ensuring appropriate handling of personal information received from the EU based on an adequacy decision by a personal information handling business operator and proper and effective implementation of the obligations laid down in such rules (*1).

In particular, Article 6 of the Act provides for the power to take necessary legislative and other action with a view to ensure the enhanced protection of personal information and construct an internationally conformable system concerning personal information through stricter rules that supplement and go beyond those laid down in the Act and the Cabinet Order. Therefore, the Personal Information Protection Commission, as the authority competent for governing the overall administration of the Act, has the power to establish pursuant to Article 6 of the Act stricter regulations by formulating the present Supplementary Rules providing for a higher level of protection of an individual's rights and interests regarding the handling of personal data received from the EU based on an adequacy decision, including with respect to the definition of special care-required personal information pursuant to Article 2, paragraph (3), of the Act and retained personal data pursuant to Article 2, paragraph (7), of the Act (including as to the relevant retention period).

On this basis, the Supplementary Rules are binding on a personal information handling business operator that receives personal data transferred from the EU based on an adequacy decision which is thus required to comply with them. As legally binding rules, any rights and obligations are enforceable by the Personal Information Protection Commission in the same way as the provisions of the Act that they supplement with stricter and/or more detailed rules. In case of infringement of the rights and obligations resulting from the Supplementary Rules, individuals can also obtain redress from courts in the same way as with respect to the provisions of the Act that they supplement with stricter and/or more detailed rules.

As regards enforcement by the Personal Information Protection Commission, in case a personal information handling business operator does not comply with one or several obligations under the Supplementary Rules, the Personal Information Protection Commission has the power to adopt measures pursuant to Article 42 of the Act. Regarding generally personal information received from the EU based on an adequacy decision, failure by a personal information handling business operator to take action in line with a recommendation received pursuant to Article 42, paragraph (1), of the Act, without legitimate ground (*2), is considered as a serious infringement of an imminent nature of an individual's rights and interests within the meaning of Article 42, paragraph (2), of the Act.

(*1) Article 4, Article 6, Article 8, Article 24, Article 60 and Article 78 of the Act, and Article 11 of the Rules.

(*2) Legitimate ground shall be understood as meaning an event of an extraordinary nature outside the control of the personal information handling business operator which cannot be reasonably foreseen (for example, natural disasters) or when the necessity to take action concerning a recommendation issued by the Personal Information Protection Commission pursuant to Article 42, paragraph (1), of the Act has disappeared because the personal information handling business operator has taken alternative action that fully remedies the violation

(1) Special care-required personal information (Article 2, paragraph (3) of the Act)

Article 2 (paragraph 3) of the Act

(3) Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

Article 2 of the Cabinet Order

Those descriptions etc. prescribed by cabinet order under Article 2, paragraph (3) of the Act shall be those descriptions etc. which contain any of those matters set forth in the following (excluding those falling under a principal's medical record or criminal history)

(i) the fact of having physical disabilities, intellectual disabilities, mental disabilities (including developmental disabilities), or other physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission;

(ii) the results of a medical check-up or other examination (hereinafter referred to as a "medical check-up etc." in the succeeding item) for the prevention and early detection of a disease conducted on a principal by a medical doctor or other person engaged in duties related to medicine (hereinafter referred to as a "doctor etc." in the succeeding item);

(iii) the fact that guidance for the improvement of the mental and physical conditions, or medical care or prescription has been given to a principal by a doctor etc. based on the results of a medical check-up etc. or for reason of disease, injury or other mental and physical changes;

(iv) the fact that an arrest, search, seizure, detention, institution of prosecution or other procedures related to a criminal case have been carried out against a principal as a suspect or defendant;

(v) the fact that an investigation, measure for observation and protection, hearing and decision, protective measure or other procedures related to a juvenile protection case have been carried out against a principal as a

juvenile delinquent or a person suspected thereof under Article 3, paragraph (1) of the Juvenile Act.

Article 5 of the Rules

Physical and mental functional disabilities prescribed by rules of the Personal Information Protection Commission under Article 2, item (i) of the Order shall be those disabilities set forth in the following.

(i) physical disabilities set forth in an appended table of the Act for Welfare of Persons with Physical Disabilities (Act No.283 of 1949)

(ii) intellectual disabilities referred to under the Act for the Welfare of Persons with Intellectual Disabilities (Act No.37 of 1960)

(iii) mental disabilities referred to under the Act for the Mental Health and Welfare of the Persons with Mental Disabilities (Act No.123 of 1950) (including developmental disabilities prescribed in Article 2, paragraph (1) of the Act on Support for Persons with Development Disabilities, and excluding intellectual disabilities under the Act for the Welfare of Persons with Intellectual Disabilities)

(iv) a disease with no cure methods established thereof or other peculiar diseases of which the severity by those prescribed by cabinet order under Article 4, paragraph (1) of the Act on Comprehensive Support for Daily and Social Lives of Persons with Disabilities (Act No. 123 of 2005) is equivalent to those prescribed by the Minister of Health, Labor and Welfare under the said paragraph

If personal data received from the EU based on an adequacy decision contains data concerning a natural person's sex life or sexual orientation or trade-union membership, which are defined as special categories of personal data under the GDPR, personal information handling business operators are required to handle that personal data in the same manner as special care-required personal information within the meaning of Article 2, paragraph (3) of the Act.

(2) Retained personal data (Article 2, paragraph (7) of the Act)

Article 2 (paragraph 7) of the Act

(7) "Retained personal data" in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by Cabinet Order.

Article 4 of the Cabinet Order

Those prescribed by cabinet order under Article 2, paragraph (7) shall be those set forth in the following.

(i) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would harm a principal or third party's life, body or fortune;

(ii) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would encourage or induce an illegal or unjust act;

(iii) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would undermine national security, destroy a trust relationship with a foreign country or international organization, or suffer disadvantage in negotiations with a foreign country or international organization;

(iv) those in relation to which there is a possibility that if the presence or absence of the said personal data is made known, it would hinder the maintenance of public safety and order such as the prevention, suppression or investigation of a crime.

Article 5 of the Cabinet Order

A period prescribed by Cabinet Order under Article 2, paragraph (7) of the Act shall be six months.

Personal data received from the EU based on an adequacy decision is required to be handled as retained personal data within the meaning of Article 2, paragraph (7) of the Act, irrespective of the period within which it is set to be deleted.

If personal data received from the EU based on an adequacy decision falls within the scope of personal data prescribed by Cabinet Order as being "likely to harm the public or other interests if their presence or absence is made known," such data is not required to be handled as retained personal data (see Article 4 of the Cabinet Order; General Rules Guidelines, "2-7. Retained personal data").

(3) Specifying a utilization purpose, restriction due to a utilization purpose (Article 15, paragraph (1), Article 16, paragraph (1) and Article 26, paragraphs (1) and (3) of the Act)

Article 15 (paragraph 1) of the Act

(1) A personal information handling business operator shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a “utilization purpose”) as explicitly as possible.

Article 16 (paragraph 1) of the Act

(1) A personal information handling business operator shall not handle personal information without obtaining in advance a principal’s consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

Article 26 (paragraphs 1 and 3) of the Act

(1) A personal information handling business operator shall, when receiving the provision of personal data from a third party, confirm those matters set forth in the following pursuant to rules of the Personal Information Protection Commission. (omitted)

(i) (omitted)

(ii) circumstances under which the said personal data was acquired by the said third party

(3) A personal information handling business operator shall, when having confirmed pursuant to the provisions of paragraph (1), keep a record pursuant to rules of the Personal Information Protection Commission on the date when it received the provision of personal data, a matter concerning the said confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

If personal information handling business operators handle personal information beyond the necessary scope to achieve a utilization purpose specified under Article 15, paragraph (1) of the Act, they shall obtain the relevant principal's consent in advance (Article 16, paragraph (1) of the Act). When

receiving the provision of personal data from a third party, personal information handling business operators shall, pursuant to the Rules, confirm matters such as the circumstances under which the said personal data was acquired by the said third party, and record these matters (Article 26, paragraphs (1) and (3) of the Act).

In the case where a personal information handling business operator receives personal data from the EU based on an adequacy decision, the circumstances regarding the acquisition of the said personal data which shall be confirmed and recorded as prescribed by Article 26, paragraphs (1) and (3), include the utilization purpose for which it was received from the EU.

Similarly, in the case where a personal information handling business operator receives from another personal information handling business operator personal data previously transferred from the EU based on an adequacy decision, the circumstances regarding the acquisition of the said personal data which shall be confirmed and recorded as prescribed by Article 26, paragraphs (1) and (3), include the utilization purpose for which it was received.

In the above-mentioned cases, the personal information handling business operator is required to specify the purpose of utilizing the said personal data within the scope of the utilization purpose for which the data was originally or subsequently received, as confirmed and recorded pursuant to Article 26, paragraphs (1) and (3), and utilize that data within the said scope (as prescribed by Articles 15, paragraph (1) and Article 16, paragraph (1) of the Act).

(4) Restriction on provision to a third party in a foreign country (Article 24 of the Act; Article 11-2 of the Rules)

Article 24 of the Act

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

Article 11-2 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 24 of the Act are to be falling under any of each following item.

(i) a personal information handling business operator and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method

(ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information

A personal information handling business operator, in cases of providing a third party in a foreign country with personal data that it has received from the EU based on an adequacy decision, shall obtain in advance a principal's consent to the effect that he or she approves the provision to a third party in a foreign country pursuant to Article 24 of the Act, after having been provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent, excluding the cases falling under one of the following (i) through (iii).

(i) when the third party is in a country prescribed by the Rules as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests

(ii) when a personal information handling business operator and the third party who receives the provision of personal data have, in relation to the handling of personal data by the third party, implemented together measures providing an equivalent level of protection to the Act, read together with the present Guidelines, by an appropriate and reasonable method (meaning a contract, other forms of binding agreements, or binding arrangements within a corporate group).

(iii) in cases falling under each item of Article 23, paragraph (1) of the Act

(5) Anonymously processed information (Article 2, paragraph 9 and Article 36, paragraphs (1) and (2) of the Act)

Article 2 (paragraph 9) of the Act

(9) "Anonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

(i) personal information falling under paragraph (1), item (i);

Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

(ii) personal information falling under paragraph (1), item (ii);

Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

Article 36 (paragraph 1) of the Act

(1) A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

Article 19 of the Rules

Standards prescribed by rules of the Personal Information Protection Commission under Article 36, paragraph (1) of the Act shall be as follows.

(i) deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (including replacing such descriptions etc. with other descriptions etc. using a method with

no regularity that can restore the whole or part of descriptions etc.)

(ii) deleting all individual identification codes contained in personal information (including replacing such codes with other descriptions etc. using a method with no regularity that can restore the individual identification codes)

(iii) deleting those codes (limited to those codes linking mutually plural information being actually handled by a personal information handling business operator) which link personal information and information obtained by having taken measures against the personal information (including replacing the said codes with those other codes which cannot link the said personal information and information obtained by having taken measures against the said personal information using a method with no regularity that can restore the said codes)

(iv) deleting idiosyncratic descriptions etc. (including replacing such descriptions etc. with other descriptions etc. using a method with no regularity that can restore the idiosyncratic descriptions etc.)

(v) besides action set forth in each preceding item, taking appropriate action based on the results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information and descriptions etc. contained in other personal information constituting the personal information database etc. that encompass the said personal information

Article 36 (paragraph 2) of the Act

(2) A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

Article 20 of the Rules

Standards prescribed by rules of the Personal Information Protection

Commission under Article 36, paragraph (2) of the Act shall be as follows.

(i) defining clearly the authority and responsibility of a person handling information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) (limited to those which can restore the personal information by use of such relating information) (hereinafter referred to as “processing method etc. related information” in this Article.)

(ii) establishing rules and procedures on the handling of processing method etc. related information, handling appropriately processing method etc. related information in accordance with the rules and procedures, evaluating the handling situation, and based on such evaluation results, taking necessary action to seek improvement

(iii) taking necessary and appropriate action to prevent a person with no legitimate authority to handle processing method etc. related information from handling the processing method etc. related information

Personal information received from the EU based on an adequacy decision shall only be considered anonymously processed information within the meaning of Article 2, paragraph (9) of the Act if the personal information handling business operator takes measures that make the de-identification of the individual irreversible for anyone including by deleting processing method etc. related information (meaning information relating to those descriptions etc. and individual identification codes which were deleted from personal information used to produce anonymously processed information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1) of the Act (limited to those which can restore the personal information by use of such relating information)).

Opinion of the Board (Art. 70.1.s)

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

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.

ARTICLE I
DECLARATION OF RIGHTS

Editor's Note
The amendment ratified by 1971 Act No 276 (1971 (57) 315) revised and rewrote this article, substituting present Section Section 1 to 23 for former Section Section 1 to 29. The amendment also transferred and renumbered the following sections of the former article: former Section 3 was transferred and renumbered as Section 1A of Article III; former Section 6 was transferred and renumbered as Section 3A of Article X; former Section 7 was transferred and renumbered as Section 3B of Article X; former Section 11 was transferred and renumbered as Section 1B of Article XVII; former Section 28 was transferred and renumbered as Section 4 of Article XIV. The provisions of former Section 9 of this article now appear in Section 1 of Article II, as amended by amendment ratified by 1971 Act No 277 (1971 (57) 319).

SECTION 1. Political power in people.
All political power is vested in and derived from the people only, therefore, they have the right at all times to modify their form of government. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 1 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see former Art I, Section 1.

SECTION 2. Religious freedom; freedom of speech; right of assembly and petition.
The General Assembly shall make no law respecting an establishment of religion or prohibiting the free exercise thereof, or abridging the freedom of speech or of the press; or the right of the people peaceably to assemble and to petition the government or any department thereof for a redress of grievances. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 4 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section Section 6, 7, 9, 10.

SECTION 3. Privileges and immunities; due process; equal protection of laws.
The privileges and immunities of citizens of this State and of the United States under this Constitution shall not be abridged, nor shall any person be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 5 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 12.

SECTION 4. Attainder; ex post facto laws; impairment of contracts; titles; effect of conviction.
No bill of attainder, ex post facto law, law impairing the obligation of contracts, nor law granting any title of nobility or hereditary emolument, shall be passed, and no conviction shall work corruption of blood or forfeiture of estate. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 8 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art 1, Section Section 4, 21.

SECTION 5. Elections, free and open.

All elections shall be free and open, and every inhabitant of this State possessing the qualifications provided for in this Constitution shall have an equal right to elect officers and be elected to fill public office. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 10 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 31.

SECTION 6. Residence.
Temporary absence from the State shall not forfeit a residence once obtained. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 12 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 35.

SECTION 7. Suspension of laws.
The power to suspend the laws shall be exercised only by the General Assembly or by its authority in particular cases expressly provided for by it. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are similar to former Section 13 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 24.

SECTION 8. Separation of powers.
In the government of this State, the legislative, executive, and judicial powers of the government shall be forever separate and distinct from each other, and no person or persons exercising the functions of one of said departments shall assume or discharge the duties of any other. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 14 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 26.

SECTION 9. Courts; speedy remedy.
All courts shall be public, and every person shall have speedy remedy therein for wrongs sustained. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 15 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 15.

SECTION 10. Searches and seizures; invasions of privacy.
The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are similar to former Section 16 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 22.

SECTION 11. Presentment or indictment.

No person may be held to answer for any crime the jurisdiction over which is not within the magistrate's court, unless on a presentment or indictment of a grand jury of the county where the crime has been committed, except in cases arising in the land or naval forces or in the militia when in actual service in time of war or public danger. The General Assembly may provide for the waiver of an indictment by the accused. Nothing contained in this Constitution is deemed to limit or prohibit the establishment by the General Assembly of a state grand jury with the authority to return indictments irrespective of the county where the crime has been committed and that other authority, including procedure, as the General Assembly may provide. (1970 (56) 2684; 1971 (57) 315; 1989 Act No. 5; 1989 Act No. 8.)

Editor's Note

The present provisions of this section are similar to former Section 17 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art 1, Section Section 18, 23.

SECTION 12. Double jeopardy; self-incrimination.

No person shall be subject for the same offense to be twice put in jeopardy of life or liberty, nor shall any person be compelled in any criminal case to be a witness against himself. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note

The present provisions of this section are similar to former Section 17 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art 1, Section Section 18, 23.

SECTION 13. Taking private property; economic development; remedy of blight.

(A) Except as otherwise provided in this Constitution, private property shall not be taken for private use without the consent of the owner, nor for public use without just compensation being first made for the property. Private property must not be condemned by eminent domain for any purpose or benefit including, but not limited to, the purpose or benefit of economic development, unless the condemnation is for public use.

(B) For the limited purpose of the remedy of blight, the General Assembly may provide by law that private property constituting a danger to the safety and health of the community by reason of lack of ventilation, light, and sanitary facilities, dilapidation, deleterious land use, or any combination of these factors may be condemned by eminent domain without the consent of the owner and put to a public use or private use if just compensation is first made for the property. (1970 (56) 2684; 1971 (57) 315; 2007 Act No. 15.)

Editor's Note

The present provisions of this section are similar to former Section 17 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section Section 18, 23.

SECTION 14. Trial by jury; witnesses; defense.

The right of trial by jury shall be preserved inviolate. Any person charged with an offense shall enjoy the right to a speedy and public trial by an impartial jury; to be fully informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to be fully heard in his defense by himself or by his counsel or by both. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are similar to former Section Section 18 and 25 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section Section 11, 13.

SECTION 15. Right of bail; excessive bail; cruel or unusual or corporal punishment; detention of witnesses.

All persons shall be, before conviction, bailable by sufficient sureties, but bail may be denied to persons charged with capital offenses or offenses punishable by life imprisonment, or with violent offenses defined by the General Assembly, giving due weight to the evidence and to the nature and circumstances of the event. Excessive bail shall not be required, nor shall excessive fines be imposed, nor shall cruel, nor corporal, nor unusual punishment be inflicted, nor shall witnesses be unreasonably detained. (1970 (56) 2684; 1971 (57) 315; 1998 Act No. 259.)

SECTION 16. Libel.

In all indictments or prosecutions for libel, the truth of the alleged libel may be given in evidence, and the jury shall be the judges of the law and facts. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 21 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 8.

SECTION 17. Treason.

Treason against the State shall consist alone in levying war or in giving aid and comfort to enemies against the State. No person shall be held guilty of treason, except upon testimony of at least two witnesses to the same overt act, or upon confession in open court. (1970 (56) 2684; 1971 (57) 315; 2007 Act No. 15.)

Editor's Note
The present provisions of the first paragraph of this section are identical to former Section 22 of Article I as it existed prior to the 1971 revision. It would seem that the intention of the 1973 amendments relating to slum clearance (1970 (57) 1340; 1973 (58) 123) was to add the provisos of the second and third paragraphs of this section to Section 17 of this article as it existed prior to the 1971 revision. Similar paragraphs were transferred to Section 5 of Article XIV by the 1971 amendment which revised this article.

SECTION 18. Suspension of habeas corpus.

The privilege of the writ of habeas corpus shall not be suspended unless when, in case of insurrection, rebellion or invasion, the public safety may require it. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 23 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 17.

SECTION 19. Imprisonment for debt.

No person shall be imprisoned for debt except in cases of fraud. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 24 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 20.

SECTION 20. Right to keep and bear arms; armies; military power subordinate to civil authority; how soldiers quartered.

A well regulated militia being necessary to the security of a free State, the right of the people to keep and bear arms shall not be infringed. As, in times of peace, armies are dangerous to liberty, they shall not be maintained without the consent of the General Assembly. The military power of the State shall always be held in subordination to the civil authority and be governed by it. No soldier shall in time of peace be quartered in any house without the consent of the owner nor in time of war but in the manner prescribed by law. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 26 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section Section 28, 29.

SECTION 21. Martial law.

No person shall in any case be subject to martial law or to any pains or penalties by virtue of that law, except those employed in the armed forces of the United States, and except the militia in actual service, but by the authority of the General Assembly. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are similar to former Section 27 of Article I as it existed prior to the 1971 revision. For similar provisions in Constitution of 1868, see Const 1868, Art I, Section 25.

SECTION 22. Procedure before administrative agencies; judicial review.

No person shall be finally bound by a judicial or quasi-judicial decision of an administrative agency affecting private rights except on due notice and an opportunity to be heard; nor shall he be subject to the same person for both prosecution and adjudication; nor shall he be deprived of liberty or property unless by a mode of procedure prescribed by the General Assembly, and he shall have in all such instances the right to judicial review. (1970 (56) 2684; 1971 (57) 315.)

SECTION 23. Provisions of Constitution mandatory.

The provisions of the Constitution shall be taken, deemed, and construed to be mandatory and prohibitory, and not merely directory, except where expressly made directory or permissory by its own terms. (1970 (56) 2684; 1971 (57) 315.)

Editor's Note
The present provisions of this section are identical to former Section 29 of Article I as it existed prior to the 1971 revision.

SECTION 24. Victims' Bill of Rights.

(A) To preserve and protect victims' rights to justice and due process regardless of race, sex, age, religion, or economic status, victims of crime have the right to:

(1) be treated with fairness, respect, and dignity, and to be free from intimidation, harassment, or abuse, throughout the criminal and juvenile justice process, and informed of the victim's constitutional rights, provided by statute;

(2) be reasonably informed when the accused or convicted person is arrested, released from custody, or has escaped;

(3) be informed of and present at any criminal proceedings which are dispositive of the charges where the defendant has the right to be present;

(4) be reasonably informed of and be allowed to submit either a written or oral statement at all hearings affecting bond or bail;

(5) be heard at any proceeding involving a post-arrest release decision, a plea, or sentencing;

(6) be reasonably protected from the accused or persons acting on his behalf throughout the criminal justice process;

(7) confer with the prosecution, after the crime against the victim has been charged, before the trial or before any disposition and informed of the disposition;

(8) have reasonable access after the conclusion of the criminal investigation to all documents relating to the crime against the victim before trial;

(9) receive prompt and full restitution from the person or persons convicted of the criminal conduct that caused the victim's loss or injury, including both adult and juvenile offenders;

(10) be informed of any proceeding when any post-conviction action is being considered, and be present at any post-conviction hearing involving a post-conviction release decision;

(11) a reasonable disposition and prompt and final conclusion of the case;

(12) have all rules governing criminal procedure and the admissibility of evidence in all criminal proceedings protect victims' rights and have these rules subject to amendment or repeal by the legislature to ensure protection of these rights.

(B) Nothing in this section creates a civil cause of action on behalf of any person against any public employee, public agency, the State, or any agency responsible for the enforcement of rights and provision of services contained in this section. The rights created in this section may be subject to a writ of mandamus, to be issued by any justice of the Supreme Court or circuit court judge to require compliance by any public employee, public agency, the State, or any agency responsible for the enforcement of the rights and provisions of these services contained in this section, and a wilful failure to comply with a writ of mandamus is punishable as contempt.

(C) For purposes of this section:

(1) A victim's exercise of any right granted by this section is not grounds for dismissing any criminal proceeding or setting aside any conviction or sentence.

(2) "Victim" means a person who suffers direct or threatened physical, psychological, or financial harm as the result of the commission or attempted commission of a crime against him. The term "victim" also includes the person's spouse, parent, child, or lawful representative of a crime victim who is deceased, who is a minor or who is incompetent or who was a homicide victim or who is physically or psychologically incapacitated.

(3) The General Assembly has the authority to enact substantive and procedural laws to define, implement, preserve, and protect the rights guaranteed to victims by this section, including the authority to extend any of these rights to juvenile proceedings.

(4) The enumeration in the Constitution of certain rights for victims shall not be construed to deny or disparage others granted by the General Assembly or retained by victims. (1998 Act No. 259.)

SECTION 25. Hunting and fishing.

The traditions of hunting and fishing are valuable parts of the state's heritage, important for conservation, and a protected means of managing nonthreatened wildlife. The citizens of this State have the right to hunt, fish, and harvest wildlife traditionally pursued, subject to laws and regulations promoting sound wildlife conservation and management as prescribed by the General Assembly. Nothing in this section shall be construed to abrogate any private property rights, existing state laws or regulations, or the state's sovereignty over its natural resources.

HISTORY: 2011 Act No. 20, Section 1, eff May 5, 2011.

Editor's Note

2011 Act No. 20, Section 1, provides in part:

"SECTION 1. The amendment to Article I of the Constitution of South Carolina, 1895, prepared under the terms of Joint Resolution 3483 of 2009, having been submitted to the qualified electors at the General Election of 2010 as prescribed in Section 1, Article XVI of the Constitution of South Carolina, 1895, and a

favorable vote having been received on the amendment, is ratified and declared to be a part of the constitution so that Article I is amended by adding Section 25:”

18/EN

WP 254 rev.01

Article 29 Working Party

Adequacy Referential

Adopted on 6 February 2018

As last Revised and Adopted on 28 November 2017

Introduction

The Working Party of EU Data Protection Authorities[1] (the WP29) has previously published a Working Document on transfers of personal data to third countries (WP12)[2]. With the replacement of the Directive by the EU General Data Protection Regulation (GDPR)[3], WP29 is revisiting WP12, its earlier guidance, to update it in the context of the new legislation and recent case law of the European Court of Justice (CJEU)[4].

This working document seeks to update Chapter One of WP12 relating to the central question of adequate level of data protection in a third country, a territory or one or more specified sectors within that third country or in an international organization (hereafter: "third countries or international organizations"). This document will be continuously reviewed and if necessary updated in the coming years, based on the practical experience gained through the application of the GDPR. Chapters 2 (*Applying the approach to countries that have ratified Convention 108*) and 3 (*Applying the approach to industry self-regulation*) of the WP12 document should be updated at a later stage.

This working paper is focused solely on adequacy decisions, which are implementing acts[5] of the European Commission, according to article 45 of the GDPR. Other aspects of transfers of personal data to third countries and international organizations will be examined in following working papers that will be published separately (BCRs, derogations).

This document aims to provide guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations by establishing the core data protection principles that have to be present in a third country legal framework or an international organization in order to ensure essential equivalence with the EU framework. In addition, it may guide third countries and international organizations interested in obtaining adequacy. However, the principles set out in this working document are not addressed directly to data controllers or data processors.

The present document consists of 4 Chapters:

Chapter 1: Some broad information in relation to the concept on adequacy

Chapter 2: Procedural aspects for adequacy findings under the GDPR

Chapter 3: General Data Protection Principles. This chapter includes the core general data protection principles to ensure that the level of data protection in a third country or international organization is essentially equivalent to the one established by the EU legislation.

Chapter 4: Essential guarantees for law enforcement and national security access to limit the interferences to fundamental rights. This Chapter includes the essential guarantees for law enforcement and national security access following the CJEU Schrems judgment in 2015 and based on the Essential Guarantees WP29 working document adopted in 2016.

---

[1] As established under Article 29 of the EU Data Protection Directive 95/46/EC

2 WP12 , 'Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' adopted by the Working Part on 24 July 1998.

3 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 (General Data Protection Regulation) (Text with EEA relevance)

4 Including Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015

[5] See relevant articles 45(3) and 93(2) of the GDPR for further information on the implementing acts

Chapter 1: Some broad information in relation to the concept of adequacy

Article 45, paragraph (1) of the GDPR sets out the principle that data transfers to a third country or international organization shall only take place if the third country, territory or one or more specified sectors within that third country or the international organization in question, ensures an adequate level of protection.

This concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. At this point it is important to recall the 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]*"[6]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.

The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States[7] that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union[8]. 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.

Article 45, paragraph (2) of the GDPR, establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organization.

For example, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organization has entered into.

It is therefore clear that any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application. It is upon the European Commission to verify – on a regular basis - that the rules in place are effective in practice.

The 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the EU Charter of Fundamental Rights and the GDPR. In addition, consideration should also be given to other international agreements on data protection, e.g. Convention 108.[9]

Attention must also be paid to the legal framework for the access of public authorities to personal data. Further guidance on this is provided in Working paper 237 (i.e. the Essential Guarantees document)[10] on safeguards in the context of surveillance.

General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to

---

[6] Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74);

[7] Article 288 (2) TFEU

[8] Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 52);

9 Recital 105 of the GDPR

[10] 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), 16/EN WP 237, 13 April 2016

data protection must be included in the third country's or international organization's legal framework. These provisions have to be enforceable.

Chapter 2: Procedural aspects for adequacy findings under the GDPR

For the EDPB to fulfil its task in advising the European Commission according to Article 70(1) (s) of the GDPR the EDPB should be provided with relevant documentation, including relevant correspondence and the findings made by the European Commission. Where the legal framework is complex, this should include any report prepared on the data protection level of the third country or international organization. In any case, 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. The EDPB will provide an opinion on the European Commission's findings in due time and, identify insufficiencies in the adequacy framework, if any. The EDPB will also endeavor to propose alterations or amendments to address possible insufficiencies.

According to Article 45 (4) of the GDPR it is upon the European Commission to monitor – on an ongoing basis - developments that could affect the functioning of an adequacy decision.

Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. This is, however, 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.

Given the mandate to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organization by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization. The EDPB would appreciate to be invited to participate in these review processes and missions.

It should also be noted that according to article 45 (5) of the GDPR the European Commission has the right to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend should consequently involve the EDPB by requesting its opinion pursuant art. 70(1) (s).

Furthermore, as now recognized in article 58 (5) of the GDPR and according to the CJEU's Schrems ruling, data protection authorities must be able to engage in legal proceedings if they find a claim by a person against an adequacy decision well founded: *"It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity"*[11].

[11] Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§ 65)

Chapter 3: General Data Protection Principles to ensure that the level of protection in a third country, territory or one or more specified sectors within that third country or international organization is essentially equivalent to the one guaranteed by the EU legislation

A third country's or international organisation's system must contain the following basic content and procedural/enforcement data protection principles and mechanisms:

A. Content Principles:

1) Concepts

Basic data protection concepts and/or principles should exist. These do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data".

2) Grounds for lawful and fair processing for legitimate purposes

Data must be processed in a lawful, fair and legitimate manner.

The legitimate bases, 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.

3) The purpose limitation principle

Data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

4) The data quality and proportionality principle

Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

5) Data Retention principle

Data should, as a general rule, be kept for no longer than is necessary for the purposes for which the personal data is processed.

6) The security and confidentiality principle

Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.

7) The transparency principle

Each individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise**,** transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

8) The right of access, rectification, erasure and objection

The data subject should have the right to obtain confirmation about whether or not data processing concerning him / her is taking place as well as access his/her data, including obtaining a copy of all data relating to him/her that are processed.

The data subject should have the right to obtain rectification of his/her data as appropriate, for specified reasons, for example, where they are shown to be inaccurate or incomplete and erasure of his/her personal data when for example their processing is no longer necessary or unlawful.

The data subject should also have the right to object on compelling legitimate grounds relating to his/her particular situation, at any time, to the processing of his/her data under specific conditions established in the third country legal framework. In the GDPR, for example, such conditions include when the processing is necessary for the performance of a task carried out in the public interest or when it is necessary for the exercise of official authority vested in the controller or when the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

The exercise of those rights should not be excessively cumbersome for the data subject. Possible restrictions to these rights could exist for example to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

9) Restrictions on onward transfers

Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.

B. <u>Examples of additional content principles to be applied to specific types of processing:</u>

1) Special categories of data

Specific safeguards should exist where 'special categories of data are involved[12]. These categories should reflect those enshrined in Article 9 and 10 of the GDPR. This protection should be put in place, through more demanding requirements for the data processing such as for example, that the data subject gives his/her explicit consent for the processing or through additional security measures.

[12] Such special categories are also known as "sensitive data" in recital 10 of the GDPR.

2) Direct marketing

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.

3) Automated decision making and profiling

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. In the European framework, such conditions include, for example, the need to obtain the explicit consent 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. 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.

C. Procedural and Enforcement Mechanisms:

Although the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those employed within the European Union[13], a system consistent with the European one must be characterized by the existence of the following elements:

1) Competent Independent Supervisory Authority

One or more independent supervisory authorities, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations.

2) The data protection system must ensure a good level of compliance

A third country system should ensure a high degree of accountability and of awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials**.**

3) Accountability

A third country data protection framework should oblige data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in

[13] Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, para. 74.

particular to the competent supervisory authority. Such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.

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

The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.

Where rules are not complied with, the data subject should be provided as well with effective administrative and judicial redress, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

Chapter 4: Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights

When assessing the adequacy of the level of protection, under Art 45(2)(a) the Commission is required to take into account "*relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data as well as the implementation of such legislation…*".

The CJEU in Schrems, noted that the "*term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter*". Even though the means to which that third country has recourse, in this connection, may differ from those employed within the European Union, those means must nevertheless prove, in practice, effective[14].

In this context, the court also noted critically that the previous Safe Harbor decision did "*not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security.*"

The WP29 has identified in the opinion WP237, adopted on 13 April 2016, essential guarantees reflecting the jurisprudence of the CJEU and the ECHR in the field of surveillance. While the recommendations detailed in WP237 remain valid and should be taken into account when assessing the adequacy of a third country in the field of surveillance, the application of these guarantees may differ in the fields of law enforcement and national security access to data. Still those four guarantees need to be respected for access to data, whether for national security purposes or for law enforcement purposes, by all third countries in order to be considered adequate:

1) **Processing should be based on clear, precise and accessible rules (legal basis)**

2) **Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated**

3) **The processing has to be subject to independent oversight**

4) **Effective remedies need to be available to the individuals**

[14] See recital 74 of Case C-360/14 "Schrems"