European Parliament
2014-2019

Plenary sitting

B8-0561/2018

10.12.2018

MOTION FOR A RESOLUTION

to wind up the debate on the statement by the Commission

pursuant to Rule 123(2) of the Rules of Procedure

on the adequacy of the protection of personal data afforded by Japan (2018/2979(RSP))

Claude Moraes
on behalf of the Committee on Civil Liberties, Justice and Home Affairs

B8-0561/2018

European Parliament resolution on the adequacy of the protection of personal data afforded by Japan
(2018/2979(RSP))

The European Parliament,

– having regard to the Treaty on European Union (TEU), the Treaty on the Functioning of the European Union (TFEU) and Articles 6, 7, 8, 11, 16, 47 and 52 of the Charter of Fundamental Rights of the European Union,

– having regard to 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)[1], and to other relevant European data protection acquis,

– having regard to the judgment of the European Court of Justice of 6 October 2015 in Case C-362/14 (Maximillian Schrems v Data Protection Commissioner)[2],

– having regard to the judgment of the European Court of Justice of 21 December 2016 in Joined Cases C-203/15 (Tele2 Sverige AB v Post- och telestyrelsen) and C-698/15 (Secretary of State for the Home Department v Tom Watson and Others)[3],

– having regard to its resolution of 12 December 2017 entitled 'Towards a digital trade strategy'[4],

– having regard to the Article 29 Working Party document 'Adequacy Referential' of 6 February 2018[5], which provides guidance to the Commission and the European Data Protection Board (EDPB) under the General Data Protection Regulation (GDPR) for the assessment of the level of data protection in third countries and international organisations,

– having regard to the draft Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan (COM(2018)XXXX),

– having regard to the findings of the visit to Japan in October 2017 of an ad hoc delegation of the Committee on Civil Liberties, Justice and Home Affairs, organised in the context of the adequacy negotiations in order to meet the relevant Japanese authorities and stakeholders in relation to the essential elements to be considered by the

[1] OJ L 119, 4.5.2016, p. 1.
[2] ECLI:EU:C:2015:650.
[3] ECLI:EU:C:2016:970.
[4] OJ C 369, 11.10.2018, p. 22.
[5] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108; endorsed by the EDPB at its first plenary meeting.

Commission when adopting its adequacy decision,

– having regard to Rule 123(2) of its Rules of Procedure,

A. whereas the GDPR has been applicable since 25 May 2018; whereas Article 45(2) of the GDPR establishes the elements to be taken into account by the Commission when assessing the adequacy of the level of protection in a third country or international organisation;

B. whereas the Commission must, in particular, take account of the rule of law, respect for human rights and fundamental freedoms, relevant legislation both general and sectoral, including that concerning public security, defence, national security, criminal law and access of public authorities to personal data, the existence and effective functioning of one or more independent supervisory authorities, and the international commitments that the third country or international organisation has entered into;

C. whereas the European Court of Justice, in its judgment of 6 October 2015 in Case C-362/14 (Maximillian Schrems v Data Protection Commissioner), clarified that an adequate level of protection in a third country must be understood to be 'essentially equivalent' to that guaranteed within the European Union by virtue of Directive 95/46/EC read in the light of the Charter;

D. whereas Japan is one of the EU's key trading partners, with which it has recently concluded an Economic Partnership Agreement (EPA) that enshrines shared values and principles while safeguarding the sensitivities of both partners; whereas the common recognition of fundamental rights, including privacy and data protection, constitutes an important basis for the adequacy decision which will provide the legal basis for the transfer of personal data from the EU to Japan;

E. whereas the ad hoc delegation of the Committee on Civil Liberties, Justice and Home Affairs to Japan was made aware of the interest of the Japanese authorities and stakeholders not only in the application of the new GDPR rules themselves, but also in developing a robust and high-level personal data transfer mechanism between the EU and Japan that would meet the conditions laid down by the EU legal framework in terms of a level of protection considered essentially equivalent to that afforded by the EU data protection legislation;

F. whereas transfers of personal data between the EU and Japan for commercial purposes are an important element of EU-Japan relations in light of the ever-increasing digitisation of the global economy; whereas such transfers should be carried out on a basis of full respect of the right to the protection of personal data and the right to privacy; whereas one of the basic objectives of the EU is the protection of fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union;

G. whereas the EU and Japan launched discussions in January 2017 to facilitate personal data transfers for commercial purposes by means of the first ever 'mutual adequacy finding'; whereas Parliament, in its resolution of 12 December 2017 entitled 'Towards a Digital Trade Strategy', explicitly 'recognise[d] that adequacy decisions [...] constitute a fundamental mechanism in terms of safeguarding the transfer of personal data from the EU to a third country';

H. whereas the adequacy decision for transfers of personal data to Japan would be the first such decision adopted under the new and stricter rules of the GDPR;

I. whereas Japan has recently modernised and strengthened its data protection legislation to align it with international standards, in particular with the safeguards and individual rights provided by the new European data protection legislative framework; whereas the Japanese data protection legal framework is composed of various pillars, with the Act on Protection of Personal Information (APPI) being the central piece of legislation;

J. whereas the Cabinet of Japan adopted a Cabinet Order on 12 June 2018 that delegates to the Personal Information Protection Commission (PPC), as the authority competent for administering and implementing the APPI, 'the power to take the necessary action to bridge differences of the systems and operations between Japan and the concerned foreign country based on Article 6 of the Act in view of ensuring appropriate handling of personal information received from such country'; whereas this decision stipulates that this includes the power to establish enhanced protections through the adoption by the PPC of stricter rules supplementing and going beyond those laid down in the APPI and the Cabinet Order; whereas pursuant to this decision, these stricter rules would be binding and enforceable on Japanese business operators;

K. whereas the draft Commission implementing decision on the adequate protection of personal data by Japan is accompanied by, as Annex I thereto, the Supplementary Rules adopted by the PPC on 15 June 2018, which are based on Article 6 of the APPI, which explicitly allows the PPC to adopt stricter rules, including for the purpose of facilitating international data transfers; whereas the Supplementary Rules are not yet publicly available;

L. whereas the purpose of these Supplementary Rules would be to address relevant differences between Japanese and EU data protection law with a view to ensuring appropriate handling of personal information received from the EU based on an adequacy decision, in particular regarding special care-required personal information ('sensitive data'), retained personal data, specifying a utilisation purpose, restriction due to a utilisation purpose, restriction on provision to a third party in a foreign country, and anonymously processed information;

M. whereas the Commission states that the Supplementary Rules would be legally binding on any personal information-handling business operator which receives personal data transferred from the EU on the basis of an adequacy decision and is therefore required to comply with those rules and any related rights and obligations, and that they would be enforceable by both the PPC and the Japanese courts; whereas some Japanese experts question whether the Supplementary Rules are binding;

N. whereas, in order to ensure an essentially equivalent level of protection for personal data transferred from the EU to Japan, the Supplementary Rules create additional protections to be applicable on a basis of stricter conditions or limitations for the processing of personal data transferred from the EU, for instance in the cases of special care-required personal information, onward transfers, anonymous data and purpose limitation;

O. whereas the Japanese data protection legal framework makes a distinction between

‘personal information’ and ‘personal data’ and refers, for some cases, to a specific category of personal data, namely ‘retained personal data’;

P. whereas, according to Article 2(1) of the APPI, the concept of ‘personal information’ includes any information relating to a living individual which enables the identification of that individual; whereas the definition distinguishes two categories of personal information, namely (i) individual identification codes and (ii) other personal information, whereby a specific individual can be identified; whereas the latter category includes information which by itself does not enable identification but can, when ‘readily collated’ with other information, allow the identification of a specific individual;

Q. whereas, according to Article 2(4) of the APPI, ‘personal data’ means personal information constituting a personal information database, etc; whereas Article 2(1) of the APPI specifies that the information in such databases is systematically arranged, similarly to the concept of a filing system under Article 2(1)of the GDPR; whereas according to Article 4(1) of the GDPR, ‘personal data’ means any information relating to an identified or identifiable natural person; whereas an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; whereas in order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly;

R. whereas, according to Article 2(7) of the APPI, ‘retained personal data’ means personal data which a personal information-handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilisation of, erase, or cease the third-party provision of, and which shall be neither those prescribed by cabinet order as likely to harm the public or other interest 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; whereas the Supplementary Rules align the notion of ‘retained personal data’ with the notion of ‘personal data’ to ensure that certain limitations to individual rights attached to the former will not apply to data transferred from the EU;

S. whereas the Japanese data protection law which is the object of the draft implementing decision excludes from its scope several sectors when they process personal data for specific purposes; whereas the draft implementing decision would not apply to the transfer of personal data from the EU to a recipient falling within any of the above-mentioned exceptions provided for by Japanese data protection law;

T. whereas as regards onward transfers of EU personal data from Japan to a third country, the draft implementing decision excludes the use for such onward transfers of transfer instruments that do not create a binding relationship between the Japanese data exporter and the third country’s data importer and do not guarantee the required level of protection; whereas this would be the case, for instance, for the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) system, in which Japan is a participating economy, as in that system the protections do not result from an

arrangement binding exporter and importer in the context of their bilateral relationship, and are clearly of a lower level than that guaranteed by the combination of the APPI and the Supplementary Rules;

U. whereas the draft implementing decision is also accompanied by a letter from the Minister of Justice of 14 September 2018 referring to a document drawn up by the Ministry of Justice and several ministries and agencies on ‘collection and use of personal information by Japanese public authorities for criminal law enforcement and national security purposes’, containing an overview of the legal framework applicable and providing the Commission with official representations, assurances and commitments signed at the highest ministerial and agency level, attached as Annex II to the implementing decision;

1. Takes note of the detailed analysis provided by the Commission in its draft adequacy implementing decision in relation to the safeguards, including oversight and redress mechanisms, applicable to the processing of data by commercial operators as well as to access to data by Japanese public authorities, in particular in the area of law enforcement and national security;

2. Takes note of the fact that Japan is also simultaneously preparing the recognition of the level of protection of personal data transferred from Japan to the EU pursuant to Article 23 of the APPI, which would result in the first ever ‘two-way’ adequacy finding worldwide leading to the creation of the world’s largest area of free and safe data flows;

3. Welcomes this development as an expression of the global spread of high data protection standards; points out, however, that this must not by any means lead to ‘tit-for-tat’ approaches in EU adequacy decisions; recalls that for an adequacy decision under the GDPR, the Commission must objectively assess the legal and practical situation in the third country, territory, sector or international organisation;

4. Points out that the European Court of Justice has ruled that the term ‘adequate level of protection’ does not require an identical level of protection to that guaranteed in the EU, but 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 the GDPR read in the light of the Charter;

5. Notes that the right to privacy and to the protection of personal data is guaranteed at constitutional level both in Japan and in the EU, but that a complete alignment of the rules of the EU and Japan will not be possible given the differences in constitutional structure as well as culture;

6. Takes note of the amendments to the APPI that entered into force on 30 May 2017; welcomes the substantive improvements;

7. Notes that the material scope of the adequacy finding is not sufficiently defined in Article 1 of the draft implementing decision, owing to the fact that the APPI excludes from its material scope several categories of business and processing activities; calls on the Commission to provide further and detailed clarifications on the impact of such exclusions on EU personal data transferred to Japan, and to clearly specify in Article 1

of the draft implementing decision which transfers of EU personal data are covered by the adequacy decision, indicating that for transfers of personal data by manual processing, the processing operations concerned would have to be covered where they are subject to further electronic processing in Japan;

8. Considers that, following the adoption of the amended APPI and of the GDPR in 2016, the Japanese and EU data protection systems share a high degree of convergence in terms of principles, safeguards and individual rights, as well as oversight and enforcement mechanisms; highlights, in particular, the creation of an independent supervisory authority, the PPC, through the amended APPI;

9. Notes, however, that the PPC itself finds that 'despite a high degree of convergence between the two systems, there are some relevant differences'; also notes that in order to provide for a higher level of protection for personal data transferred from the EU, the PPC adopted the Supplementary Rules on 15 June 2018;

10. Welcomes a number of important clarifications in the Supplementary Rules, including the alignment of 'anonymised personal information' in the APPI with the definition of 'anonymous information' in the GDPR;

11. Considers that the additional protections of the Supplementary Rules cover only transfers under adequacy decisions; recalls that in view of the scope of the adequacy decision, some data transfers will be conducted under these other available mechanisms;

12. Acknowledges that the additional protections stipulated in the Supplementary Rules are limited to personal data transferred from Europe, hence business operators who have to simultaneously process Japanese and European personal data will be obliged to comply with the Supplementary Rules, by ensuring, for example, technical means ('tagging') or organisational means (e.g. storing in a dedicated database) in order to be able to identify such personal data throughout their 'life cycle'; calls on the Commission to monitor the situation so as to prevent potential loopholes by which operators could circumvent the obligations laid down in the Supplementary Rules by transferring data via third countries;

13. Notes that the definition of 'personal data' in the APPI excludes data 'prescribed by cabinet order as having little possibility of harming an individual's rights and interests considering their utilisation method'; urges the Commission to assess whether this harm-based approach is compatible with the EU approach under which all processing of personal data falls within the scope of data protection law; also notes, however, that this approach would apply in very limited situations;

14. Notes further that the definition of 'personal information' in the APPI is limited to information 'whereby a specific individual can be identified'; also notes that this definition does not include the clarification provided by the GDPR that personal information should also be considered personal data when it can be merely used to 'single out' a person, as clearly established by the European Court of Justice;

15. Is concerned that the narrower definition of 'personal data' (based on the definition of 'personal information') in the APPI might not meet the standard of being 'essentially equivalent' to the GDPR and to the case law of the European Court of Justice;

questions, therefore, the statement in the draft implementing decision that ‘EU data will always fall into the category of “personal data” under the APPI’; calls on the Commission to closely monitor the practical implications of the different concepts in the course of the application of the adequacy decision and its periodic review;

16. Calls on the Commission to provide further clarifications, and if necessary to request further binding supplementary rules from the Japanese authorities, in order to ensure that all personal data in the meaning of the GDPR are protected when transferred to Japan;

17. Notes with concern that as regards automated decision-making and profiling, differently from EU law, neither the APPI nor the PPC Guidelines contain legal provisions and that only certain sectoral rules address this matter, without providing a comprehensive overall legal framework with substantial and strong protections against automated decision-making and profiling; calls on the Commission to demonstrate how this is addressed in the Japanese data protection framework in such a way as to ensure an equivalent level of protection; considers that this is especially relevant given the recent Facebook/Cambridge Analytica profiling cases;

18. Considers that in the light of the Adequacy Referential of the EDPB further in-depth clarifications are needed as regards direct marketing, given the lack of specific provisions in the APPI, in order to demonstrate the Japanese equivalent level of personal data protection;

19. Considers that regarding onward transfers, although the combination of the APPI rules and the Supplementary Rules would ensure a level of protection higher than that provided under the APEC CBPR, the solution provided in the Supplementary Rules, which consists of requiring prior consent on the part of EU data subjects for approval of onward transfer to a third party in a foreign country lacks certain essential elements that would enable data subjects to formulate their consent, as it does not expressly define what is covered by the notion of ‘information on the circumstances surrounding the transfer necessary for the [data subject] to make a decision on his/her consent’, in line with Article 13 of the GDPR, such as the third country of destination of the onward transfer; notes that in addition, the draft implementing decision does not explain the consequences for the data subject in case of refusal of consent for onward transfer of his or her personal data;

20. Calls on the Commission to further assess and demonstrate whether the independence of the PPC fully complies with the requirements developed through the case law of the European Court of Justice and reflected in the GDPR;

21. Regrets that, as regards effective enforcement of the APPI, the level of possible fines that would be imposed by the penal authorities is insufficient to ensure effective compliance with the Act, as it does not seem to be proportionate, effective or dissuasive in relation to the gravity of the infringement; notes, however, that the APPI also provides for criminal sanctions including imprisonment; calls on the Commission to provide information on the actual use of administrative fines and criminal sanctions in the past;

22. Takes note that while the PPC has no oversight of the data processing activities of the

law enforcement sector, other supervision mechanisms exist, including oversight by the independent Prefectural Public Safety Commission; notes that the Information Disclosure and Personal Information Protection Review Board also has some competences in this field, including reviewing access requests and publishing opinions, but points out that these powers are not legally binding; welcomes the fact that the EU and Japan have agreed to put in place a specific redress mechanism, administered and supervised by the PPC, which will apply to the processing of personal data in law enforcement and national security sectors;

23. Notes that under the Japanese Act on the Protection of Personal Information held by Administrative Organs (APPIHAO), business operators can also hand data over to law enforcement authorities on a 'voluntary basis'; points out that this is not provided for in the GDPR or the Police Directive and is concerned that it might not be compliant with the standard of being 'essentially equivalent' to the GDPR;

24. Is aware of media reports about the Japanese Directorate for Signals Intelligence (DFS), 'which employs about 1 700 people and has at least six surveillance facilities that eavesdrop around the clock on phone calls, emails, and other communications'[1]; is worried that this element of indiscriminate mass surveillance is not even mentioned in the draft implementing decision; calls on the Commission to provide more information about Japanese mass surveillance; is seriously worried that this mass surveillance will not stand the test of the criteria established by the European Court of Justice in the Schrems judgment (Case C-362/14);

25. Regrets that the document 'Collection and use of personal information by Japanese public authorities for criminal law enforcement and national security purposes', which forms part of Annex II to the draft implementing decision, does not have the same legally binding effect as the Supplementary Rules;

Conclusions

26. Calls on the Commission to provide further evidence and explanation regarding the above-mentioned matters, in order to demonstrate that the Japanese data protection legal framework ensures an adequate level of protection that is essentially equivalent to that of the European data protection legal framework;

27. Believes that this adequacy decision can, furthermore, send out a strong signal to countries around the world that convergence with the EU's high data protection standards offers very tangible results; stresses, in this regard, the importance of this adequacy decision as a precedent for future partnerships with other countries that have adopted modern data protection laws;

28. Instructs its Committee on Civil Liberties, Justice and Home Affairs to continue to monitor developments in this field, including on cases brought before the Court of Justice, and to monitor the follow-up to the recommendations made in this resolution;

[1] Ryan Gallagher, 'The Untold Story of Japan's Secret Spy Agency', The Intercept, 19 May 2018, https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/

°

° °

29. Instruct its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States, the European Data Protection Board, the European Data Protection Supervisor, the Committee established pursuant to Article 93(1) of the General Data Protection Regulation, the Council of Europe and the Government of Japan.