**Follow up to the European Parliament non-legislative resolution on the adequacy of the protection of personal data afforded by Japan**

1. **Resolution tabled pursuant to Rule 123(2) of the European Parliament's Rules of procedure by the Committee on Civil Liberties (LIBE)**
2. **Reference numbers:** 2018/2979(RSP) / B8-0561/2018 / P8\_TA-PROV(2018)0529
3. **Date of adoption of the resolution:** 12 December 2018
4. **Competent Parliamentary Committee:** Committee onCivil Liberties (LIBE)
5. **Brief analysis/ assessment of the resolution and requests made in it:**

General assessment

The resolution concerns 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. The draft was endorsed by the College on 5 September 2018 and subsequently underwent revisions following discussions with the European Data Protection Board (the opinion of which is required for the adoption of the implementing measure) and the Member States representatives in the context of the “comitology” procedure also taking into account the resolution of the European Parliament. The decision was adopted by the Commission on 23 January 2019 and became effective on the same day.

The European Parliament recalls that the adequacy decision must be, under Article 45(2) of the General Data Protection Regulation (GDPR), preceded by a thorough analysis of the relevant legal provisions of the third country concerned, as well as the “rule of law, respect for human rights and fundamental freedoms” and its international commitments. Against this background, it observes that “the common recognition of fundamental rights, including privacy and data protection, constitutes an important basis for the adequacy decision”. At the same time, it recognises that Japan is a key trading partner of the European Union and takes note of the growing importance of trans-border data flows. In this context, the European Parliament also recalls the recent conclusion of the Economic Partnership Agreement between the European Union and Japan. The European Parliament further recalls that the European Court of Justice, in its judgment of 6 October 2015 ([Schrems case](http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN)) 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, without a full identity of rules being needed.

The resolution generally welcomes the draft implementing measure, acknowledging notably its importance “as an expression of the global spread of high data protection standards”. It also takes note of the recent revision of the Japanese data protection framework and of the adoption by the Japanese government of Supplementary Rules bridging the gaps in protection as compared to the legislation of the European Union. The resolution explicitly recognises that “the Japanese and EU data protection systems share a high degree of convergence”.

Nevertheless, the resolution calls for a further assessment of certain aspects of the Japanese data protection system, clarification of individual points explained in the decision and for an increased focus in the decision on monitoring of the application of the Japanese framework.

Specific issues

The European Parliament raises questions pertaining to the **scope of the decision**, in particular as concerns the definition of ‘personal data’ in the Japanese Act on the Protection of Personal Information (APPI). More specifically, the European Parliament is concerned that the definition of ‘personal data’ in the APPI could be narrower than the one in the GDPR. It also mentions the exclusion from the scope of this definition of data “prescribed by cabinet order as having little possibility of harming an individual’s rights and interests considering their utilisation method”. The European Parliament therefore asks the Commission to further clarify these issues and “closely monitor the practical implications” of these allegedly different concepts (paragraphs 13 to 16).

Following the Opinion of the European Data Protection Board (EDPB), the European Parliament insists on the need for further clarification of the mechanism ensuring that personal data transferred from the European Union to Japan will continuously benefit from the **strengthened protections** under the Supplementary Rules “**throughout their life cycle**” (paragraph 19).

Still with reference to the Opinion of the EDPB, the European Parliament asks for additional clarifications concerning the continuity of protections included in the GDPR in cases of **automated decision-making** and **direct marketing** (paragraphs 17and 18).

The European Parliament requires further clarifications on whether, in cases of **onward transfers** (from Japan) of personal data originating from the European Union based on **consent**, the Supplementary Rules ensure that such consent can be considered as sufficiently informed. In particular, it is concerned that the notion of “information on the circumstances surrounding the transfer necessary for the data subject to make a decision on his/her consent” is not defined (paragraph 20).

The European Parliament criticises the small amounts of **fines** that may be imposed under the APPI. Although it recognises the dissuasive effect of alternative **sanctions** existing in the Japanese law, it requests further clarifications and information concerning the application of these sanctions (paragraph 21).

In the context of government access to personal data received by Japanese business operators from the European Union, the resolution refers to the fact that business operators might **provide data to law enforcement authorities on a “voluntary basis”**; the Commission is requested to further assess the compliance of such voluntary cooperation with EU law (paragraph 23).

The European Parliament raises concerns as regards alleged **surveillance activities** of the Japanese Directorate for Signals Intelligence (DFS), reported by media (paragraph 24).

With reference to **annex II** to the decision, the European Parliament regrets that the document “does not have the same legally binding effect as the Supplementary Rules” (paragraph 25).

1. **Response to requests and overview of action taken, or intended to be taken, by the Commission:**

The Commission welcomes the overall positive approach of the European Parliament to the implementing measure under consideration and fully shares its assessment that the decision concerning Japan is essential for the global promotion of high data protection standards and as a complement to the Economic Partnership Agreement. As adopted on 23 January 2019, together with the parallel adequacy finding for the European Union by Japan, it created the largest area of free and safe data flows in the world.

Prior to adoption, the Commission also duly examined the specific observations made by the European Parliament in the resolution. While it ultimately does not share the concerns, these observations were helpful as they showed where further clarifications were needed (as well as where the focus of future reviews and monitoring should be). Thus, the Commission took them into account while revising the draft of the decision and added relevant clarifications and explanations in the recitals. The revised decision also clearly identifies certain issues that should be monitored by the Commission.

As regards the **scope of the decision**, detailed explanations have been added, in particular in recitals 20 to 22 of the decision. Moreover, the recommendation of the European Parliament is followed-up by the addition of a new paragraph in the operative part (Article 3(1) providing that the Commission shall continuously monitor the application of the relevant Japanese legal framework), as well as by recital 177 on monitoring (which clarifies that this also covers the “actual practice for the processing of personal data”, thereby including the practical impact of the different concepts used in the Japanese data protection law on the protection of personal data transferred to Japan in practice).

On the continuity of strengthened **protection throughout the life cycle** of the data transferred, the concerns of the European Parliament have been addressed in recital 15 and footnote 13. Further amendments to Article 3(1), (2), recital 177 (monitoring) and recitals 180 to 183 (review) refer to appropriate follow-up of the issues mentioned in paragraph 19 of the resolution.

Concerning the continuity of protections applicable **to automated decision-making** and **direct marketing**, the Commission continues to believe that the issue is of no (or only minor) relevance in the context of international data transfers covered by the decision. Automated decisions will typically be taken by the European data exporter (which merely “outsources” processing). In the exceptional case where the Japanese data importer or any further recipient in Japan would itself take a decision directly vis-à-vis the European Union individual, it would in (almost) all cases fall directly within scope of application of GDPR pursuant to its Article 3 (2) (a) or (b) (see recital 94 and footnote 56). However, the Commission agrees that this question should be subject to monitoring. The points raised by the European Parliament have been addressed in the aforementioned Article 3 (1), (2), recital 177 (monitoring), as well as in recitals 180 to 183 on review (i.e. a commitment to carry out periodical checks whether all the findings included in the decision, hence including those concerning automated decision-making and direct marketing, “are still factually and legally justified”).

As regards the observations on **onward transfers**, the Commission recalls that adequacy does not mean identity of rules and hence, in order to be considered adequate, the provisions of the APPI and of the Supplementary Rules do not need to be identical to the relevant provisions of the GDPR. What matters under the “essential equivalence” test is that the European Union data subject will receive the information necessary to make an informed decision on whether to give his/her consent, including information on the specific country of decision (as clarified by Supplementary Rule (4)). Additional explanations and analysis have been included, along these lines, in recitals 38 and 76 of the decision. The points raised by the European Parliament have also been addressed in Article 3(1) and recital 181.

As concerns the **fines** and **other sanctions** in Japanese law, additional clarifications have been added in recitals 102 and 108 of the decision. Furthermore, this issue will be subject to continuous follow-up, as indicated in the revised Article 3(1), recitals 177 (monitoring) and 180 to 183 (review). Recital 181 refers explicitly to the review of the effectiveness of enforcement.

Regarding the **provision of data** **to law enforcement authorities** **on a “voluntary basis”**, the Commission considers that this is not at odds with the continuity of protection under Chapter V of the GDPR. Indeed, what matters is not whether the personal data are handed over to public authorities for law enforcement purposes on a voluntary basis or mandatorily, but whether any requests for voluntary disclosure are subject to sufficient safeguards (in terms of legal basis, limitations, oversight and redress). Such safeguards are indeed provided in the Japanese system (as described in recitals 125 to 150 of the decision).

In addition to the abovementioned observations that the Commission considers pertinent and that have been duly addressed, there is a small number of points made in the resolution with which the Commission would respectfully disagree.

This is the case for the media reports on the **alleged surveillance activities** of the Japanese Directorate for Signals Intelligence (DFS). These allegations are not substantiated and moreover directly contradicted by official representations and assurances provided by the Japanese government at the highest political level (see annex II to the decision). In particular, we would draw the attention to the statements included in section III.A.1) (4) (regarding the Ministry of Defence that includes the DFS) and in section III.A.2) (b) (denying the existence of any mass and indiscriminate collection or access to personal information for national security reasons) of annex II. These statements are reflected in recital 156 of the decision. The Commission would also invite the European Parliament to consider that the DFS is the intelligence agency of the Japanese military forces whose main mission is notably to monitor the radio and satellite communications, movements of ships, aircrafts of other (hostile) military forces. Those are typical military intelligence activities that are not relevant to the “adequacy scenario” (i.e. access by public authorities to data held by commercial operators that have imported it from the European Union).

As regards the lack of binding effect of **annex II**, it is important to stress that – as a document containing official representations and assurances on the rules applying to government access to data signed by various Japanese Ministers and Heads of Agencies – it is of a different nature than the Supplementary Rules (which contain rules for commercial operators based on an empowerment in the APPI).