Update to Paper Addressing Human Resources Data Flows in Light of European Data Protection Board Recommendations

Lynn Goldstein
Martin Abrams

August 2021

Key Conclusion

The European Data Protection Board (EDPB has issued guidance setting forth how risk-based decisions that balance the full range of rights and interests impacted by the transfer or non-transfer of human resource and similar personal data used for a business purpose should be conducted. Such subjective judgements are permitted if the decisions are based on objective information that is demonstrable. There is such objective information related to human resource data being transferred to the United States, and so those transfers may proceed without supplementary measures.

Background

The EDPB made recommendations in October 2020 on Supplementary Measures that took the position that only objective factors, and not subjective ones such as the likelihood of public authorities' access to personal data, could be relied upon to determine whether a third country ensures an essentially equivalent level of protection. This position made it difficult for human resource (HR) data to be transferred when the EU data exporter is a company subsidiary and the U.S. data importer is the company headquarters and when the HR data is either (1) stored in the cloud in the EU in the clear and is processed in the clear in the third country or (2) remotely accessed in the EU from the third country and the data is in the clear in the EU or the encryption key is located in the third country.

The Information Accountability Foundation (IAF) argued in its March 2021 paper Addressing Human Resource Data Flows in Light of European Data Protection Board Recommendations that by prohibiting consideration of subjective factors, and thereby making it impossible for companies to access HR data either remotely or stored in the cloud, the right to protection of personal data is prioritized over other individual rights set forth in the Charter of Fundamental Rights of the EU (Charter). In particular, EU individuals' fundamental rights to engage in work and freedoms to choose an occupation and to conduct a business are undermined and the right to protection of personal data is favored.

The New Standard Contractual Clauses

The European Commission adopted new Standard Contractual Clauses (SCCs) for transfers of personal data out of the EU to third countries that do not ensure essentially equivalent levels of protection on 4 June 2021. Clause 14, which addresses local laws and practices affecting compliance with the SCCs, requires the data exporter and data importer to warrant that laws and practices in the third country (including those governing access to personal data by public authorities) do not prevent the data importer from fulfilling its obligations under the SCCs. Footnote 12 in Clause 14 provides that, in assessing whether such a warranty can be made, "relevant and documented practical experience of prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficient time-frame" may be considered. That footnote further provides that the parties must take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of such requests within the same sector and/or the application of the law in practice.

The EDPB's Adopted Recommendations

The EDPB adopted its Recommendations on Supplemental Measures a few weeks later on 18 June. The adopted Recommendations set forth a six- step roadmap. The final Recommendations specifically permit subjective risk decisions based on objective evidence. Step three, assessment of the third-country's law and/or practices, allows, in addition to the third country's legislation, consideration of the practices of the third country's public authorities.

If the data exporter considers and is able to demonstrate and document that it has no reason to believe that relevant and "problematic legislation"[1] will be interpreted and/or applied in practice so as to cover the transferred data and the data importer, the data exporter may decide to proceed with the transfer without implementing supplementary measures. The data exporter needs to demonstrate and document through an assessment, in collaboration with the data importer where appropriate, the experience of other actors operating within the same sector and/or related to similar transferred personal data.

The documented practical experience or absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor of the effectiveness of the SCCs that allows transfer to proceed without supplementary measures. This information only will be able to be considered together with other types of information obtained from other sources as part of the assessment of the law and practices of the third country in relation to the transfer. The relevant and documented experience of the importer should be corroborated and not contradicted by relevant,[2] objective,[3] reliable,[4] verifiable,[5] and publicly available or otherwise accessible information[6] on the practical application of the relevant law (e.g., the existence or absence of requests for access received by other actors operating within the same sector and or related to similar transferred personal data and/or the application of the law in practice, such as case law and reports by independent oversight bodies.)

Use Cases 6 and 7

[1] "Problematic legislation" is defined in footnote 63 of the Adopted Recommendations as legislation that 1) imposes on the recipient of personal data from the EU obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognized by the Charter or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also raised in Union or EU Member States' law, such as those listed in Article 23(1) of the GDPR.

[2] According to Section 46 of the Adopted Recommendations, the information must be relevant to the specific transfer and/or importer and their compliance with the requirements set in EU law and the Article 46 GDPR transfer instrument, and not overly general or abstract

[3] According to Section 46 of the Adopted Recommendations, Objective Information is information that is supported by empirical evidence based on knowledge gained from the past, not assumptions about potential events and risks.

[4] According to Section 46 of the Adopted Recommendations, the exporter and importer must objectively assess the reliability of the source of information and of the information itself and evaluate them separately.

[5] According to Section 46 of the Adopted Recommendations, information and conclusions should be verifiable or contrastable with other types of information or sources, as part of an overall assessment, also to allow the competent supervisory or judicial authority to check the objectivity and reliability of this information if needed.

[6] According to the Section 46 of the Adopted Recommendation, information should preferably be public or at least accessible to facilitate the verification of the criteria made above and ensure its possible sharing with supervisory authorities, judicial authorities and ultimately data subjects.

For both Use Case 6, transfer to cloud service providers or other processors which require access to data in the clear, and Use Case 7, transfer of personal data for business purposes including by way of remote access, the EDPB, considering the current state of the art, is incapable of envisioning an effective technical measure to prevent such access from infringing on individual rights. However, the EDPB does refer to Step 3, i.e., whether there is no reason to believe that the problematic legislation will be interpreted or applied in practice so as to cover the transferred data.[7]

The EDPB's referral to Step 3 means that the data exporter can look at other objective, reliable, relevant, verifiable, and publicly available information to clarify the scope of the application in practice of the "problematic legislation" to the transfer of the personal data. This information should answer these questions:

1. Does publicly available information show there is a legal prohibition of informing about a specific request for access to data received and wide restrictions on providing general information about requests for access to data received or absence of requests received?
2. Has the importer confirmed it has or has not received requests for access to data from public authorities in the third country in the past, and if not, that it is not prohibited from providing information about such requests or their absence?
3. Does publicly available information (third country case law and reports from oversight bodies, civil society, academic organizations) reveal data importers of the same sector as the importer have or have not received requests for access to data for similar transferred data in the past?

If answers to these questions lead to the conclusion that the problematic legislation does not apply in practice, the transfer may proceed without supplementary measures.

HR Data

The IAF team interviewed almost all the companies that were interviewed for the March paper and asked them questions related to the questions in the Use Cases 6 and 7 Section. These global companies are headquartered in the U.S. and have employees in the EU and hundreds of countries. Collectively, these companies are in the pharmaceutical, hardware,

[7] Step 3 has two other alternatives when the data exporter is assessing whether legislation in a third country impinges on SCCs, i.e., whether the legislation in the third country may be problematic. If it is, the data exporter may: (1) stop the transfer, or (2) implement the supplementary measures to prevent risk of potential application to the importer and/or the transferred data of laws and/or practices of the third country. Currently, the EDPB's reference back to Step 3 cannot be referring to either of these two alternatives because alternative 1, stop the transfer, is no different than the conclusion reached by the EDPB in Use Cases 6 and 7 given its view of the current state of the art, and alternative 2, implement supplementary measures, does not work because the EDPB has concluded that under the current state of the art, there is no effective technical measure to prevent access from infringing on the data subject's fundamental rights.

software, and financial services industries. HR data either (1) is accessed in the clear remotely from the EU data exporter, a company subsidiary, by the U.S. data importer, the company's headquarters, or (2) is stored in the cloud by the EU data exporter, a company subsidiary, and is processed by the U.S. data importer, the company headquarters.

For the purposes of this paper, it is assumed that the relevant U.S. law is problematic legislation.[8] The experience of these companies is consistent with the publicly available information about the application in practice of U.S. problematic legislation. The answers of the companies to the questions in the section on Use Cases 6 and 7 are as follows:

1. There is no law that prohibits informing about the absence of the receipt of requests by public authorities for access to personal data.[9]
2. The survey of these companies, data importers who are company headquarters located in the U.S., confirmed that these data importers have not received requests for access to HR data from U.S. public authorities. The answer to Question 1 confirms that they are not prohibited from providing information about the absence of such requests.
3. The White Paper issued by the U.S. Departments of Commerce and Justice and the Office of the Director of National Intelligence,[10] states:

> "Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data.
>
> Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies. Neither would such companies have any indication that a U.S. intelligence agency has sought to obtain their data unilaterally outside the United States under the authority of EO12333.[11]

Thus, publicly available information reveals that data importers of the same sectors as these companies have not received requests for access to HR data in the past.

[8] Ian Brown & Douwe Korff, Exchanges of Personal Data after the Schrems II Judgment, Study Requested by the LIBE Committee, European Parliament, at 113 (July 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

[9] Warrant Canary Frequently Asked Questions, Is it Legal to Publish a Warrant Canary? Electronic Frontier Foundation, April 10, 2014, https://www.eff.org/deeplinks/2014/04/warrant-canary-faq

[10] Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*, September 2020, https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

[11] Id.

Since the U.S. problematic legislation does not apply in practice to HR data, the transfer of HR data to the U.S. can proceed without any supplementary measures.[12] The same questions would have to be asked and answered for every additional country that might have problematic legislation.

Conclusion

Consideration of the application in practice of the U.S. "problematic legislation" means that a risk-based approach can be taken to the transfer from the EU to a third country of HR data and other commercial information by companies who are not in the business of transmitting (or storing) communications for third parties. By considering the way the intelligence agency in the third country exercises and articulates its power, the rights and freedoms of individuals set forth in the Charter are balanced appropriately, and the right to the protection of personal data is not preferred to the disadvantage of the freedom to choose an occupation and the right to engage in work and the freedom to conduct a business.

[12] Under GDPR Article 32, appropriate technical and organisational measures, such as pseudonymisation and encryption of personal data, are required to ensure a level of security appropriate to the risk.