EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

Ms ...
Data Protection Officer
X EUI

Brussels, ... 2020
WW/.../xx/ D(20xx) xxx **C 2019-0842**

Subject: X EUI's consultation on A's cooperation (Case 2019-0842)

Dear Ms ...,

Thank you for your informal consultation under Article 41(1) of Regulation (EU) 2018/1725 (the Regulation). The subject of your consultation concerns the "gentlemen's agreement" between X EUI (X) and A, according to which X can make use of A's meeting facilities to host X meetings. This entails the processing of personal data, namely the transfer of names of the participants to A, which are necessary for security and organisational purposes.

Facts

You have pointed out that you have already done your analysis of Article 28 (whether X and A can be in a joint controllership relationship) as well as of Article 48 (transfers subject to appropriate safeguards) and you have concluded that these provisions cannot be used as they will not fit with the A's role. You have also stressed that the relationship between X and A is that of a controller-processor relationship.

You have highlighted that A is an international organisation, which applies its own rules on data protection and it is not bound by the Regulation. You have explained that "for political reasons, the conclusion of an administrative agreement between X and A defining the statute, seat and operational rules of X has not been (and will not likely be) possible". X has concluded an Exchange of Letters (EoL) at the level of Director-General for A and Chef Executive for X in order to establish their cooperation. The question you raised is to what extent an EoL could be considered as legally binding instrument fulfilling the requirements of Article 29(3) of the Regulation.

The difficulty in the present case is that, as you have pointed out, "A is an international organisation, which applies its own data protection rules and it is not bound by Regulation 2018/1725". This means that the rules on international transfers of data in Chapter V of the Regulation come into play as well.

Legal analysis

1) Controller-Processor Relationship and Distribution of Roles

We will first remind the content of a possible controller-processor relationship between X and A. The main question in hand is whether the EoL is a "contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller" as required under Article 29(3) of the Regulation.

In light of Article 29[1] of the Regulation, X, being the controller, should ensure that the arrangement with A should contain clear and precise obligations, roles and tasks of the respective parties regarding data protection; such provisions should give effect to those principles and rights, thus ensuring adequate protection of transferred personal data and effective legal remedies for the data subjects.

In particular, X should indicate in the arrangement with A the following elements:
- the responsibilities/tasks of A and of X respectively,
- the **subject-matter, duration, nature, purpose** of the processing,
- the **types of personal data** and **categories of data subjects**,
- the **retention period** of personal data and choose whether A should delete or return all the personal data to X (and delete any copies) after the end of its service,
- that X **can verify whether A is in compliance via audits** and **A should allow for and contribute to audits/inspections.**

Moreover, **X should add in the arrangement that A,**

- processes data only on the **documented instructions** from X, including with regard to transfers of personal data and to any onward transfers,
- A will take all measures required to ensure the security and confidentiality of personal data,
- **assists X** with the obligation to guarantee the **rights of data subjects** and to fulfil X's obligations as controller pursuant to Articles 33-41 of the Regulation,
- **notifies personal data breaches** within 48h to X,
- **notifies** any legally binding **request for disclosure** of the personal data processed on behalf of X and may only give access to data with the prior written authorisation of X,
- **not process data for other incompatible purposes** (X should determine what (if any) processing for compatible purposes is allowed),
- **not outsource/subcontract** the processing; if A intends to engage a sub-processor, this can be done only with the prior written authorisation of X. This means that A should inform X of any intended changes, should provide X with the necessary information on the intended sub-processor as well as on the processing it would be entrusted with and should give X the opportunity to object to / decide on the intended sub-processor. Once X grants the authorisation, A should contractually pass on to any subcontractors the same obligations as in the arrangement for the relevant part of the processing.

The arrangement should therefore not only contain the specific provisions listed above, but it should also indicate the mutually binding will and commitment of both parties to respect generally accepted internationally recognised data protection principles as well as rights and freedoms of individuals.

---

[1] See EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 (the EDPS Guidelines) available at: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf, pages 18 &19.

If X and A can agree on the above data protection rules and principles and indicate them in the EoL, then this kind of arrangement can be considered as "a contract or other legal act under Union or Member State law, that is binding on the processor" under Article 29(3) of the Regulation. If A is not willing to include in the EoL all the above, then the EoL cannot rise to the level of commitment under Article 29(3) of the Regulation.

2) Separate controllers and transfer of data

In this case, X should rather examine the possibility of framing this relationship as a transfer between two separate controllers.

The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of a controller within the meaning of the Regulation. Not every service provider that processes personal data in the course of delivering a service is a "processor" within the meaning of the Regulation. The role of a processor stems from its concrete activities in a specific context. In practice, where the provided service is not specifically targeted at processing personal data or does not constitute a sufficiently important element of the service, the service provider may be in a position to independently determine the purposes and means of that processing, which is required in order to provide the service (think for example of a taxi company: it processes personal data on request of a customer, but that processing is purely auxiliary to the transportation service provided). In that situation, the service provider can be considered as a separate controller and not as a processor[2]. The EDPB will provide additional guidance on the equivalent provisions of GDPR in upcoming guidelines.

That is why a case-by-case analysis remains necessary. Before X launches the processing, in its role as data controller, should ascertain the degree of influence that each party effectively has in determining the purposes and means of the processing. X should check and assess whether A exerts a decisive influence on the processing regarding the means of the processing.

In concrete, does A insist on applying its own rules, not those of X, regarding for instance the retention of data, which data are collected, who has access to the data within A or on the transfer of data to other entities? If the majority of the replies is yes, this might lead to the conclusion that it is A that determines the essential elements of the means of the processing[3]. If indeed the factual essential elements and circumstances qualify A as a controller, then it can be argued that there is a transfer between two separate controllers, X and A.

3) Transfer Rules

Considering that there is a transfer of personal data between two separate controllers, of which one is an international organisation, it is important to recall Article 46 of the Regulation, which lays down the general principle for international transfers[4] and it includes transfers of personal

---

[2] See also recital 81 of the GDPR, which refers to "entrusting a processor processing activities", indicating that the processing activity as such is an important part of the decision of the controller to ask a processor to process personal data on its behalf.

[3] With regard to the essential elements of the means of the processing, see:
i) The EDPS Guidelines
ii) The EDPB has drafted Guidelines on controllers, processors and joint controllership under Regulation 2016/679 and they will be adopted soon. Useful information can still be found in Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor", available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[4] For more information on the reasoning behind, please see recital 63 of the Regulation: "*the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should be guaranteed. The same guarantees should apply in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any*

data to an international organisation. The provision states that any international transfer shall take place **only if,**

i) subject to the other provisions of this Regulation,

ii) the conditions laid down in Chapter V are complied with by the controller and processor,

"The conditions laid down in Chapter V" means that Article 48(1) of the Regulation is applicable in the case at hand, because there is no adequacy decision covering A and the transfers are likely to be too structural and repetitive to qualify as a derogation under Article 50. Therefore, X may transfer personal data to A only if X has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. In the case of transfers to international organisations, the appropriate safeguards may be provided for[5] by

- signing a legally binding and enforceable instrument between an EU institution and an international organisation[6] (Article 48(2)(a) of the Regulation), or

- inserting provisions into administrative arrangements between an EU institution and an international organisation which includes enforceable and effective data subject rights. These administrative arrangements are subject to authorisation from the EDPS (Article 48(3)(b) of the Regulation).

If X and A can agree on the content of the arrangement in conformity with the safeguards under Article 48(2)(a) of the Regulation, an EoL can be considered as "a legally binding and enforceable instrument". If not, Article 48(3)(b) is left as the most appropriate option[7].

Derogations under Article 50 of the Regulation are not applicable in the case at hand, as the transfers are likely to be repeated and structural, since X regularly relies on A's facilities for meetings.

Conclusion

The EDPS points out that an administrative arrangement between two separate controllers covering international transfers under Article 48(3)(b) of the Regulation is likely the most suitable relationship between X and A in this specific case at hand. Both entities however should do more than merely restate the provisions of the Regulation in the administrative arrangement. They should further elaborate and specify them, for instance on security measures to be implemented.

---

event, transfers to third countries and international organisations may only be carried out ***in full compliance with this Regulation*** *and* ***respecting the fundamental rights and freedoms enshrined in the Charter*** [emphasis added]".

[5] Contractual clauses, whether standard ones under Article 48(2)(b) or (c) or "ad-hoc" under Article 48(3)(b) are usually not an option for international organisations, as their privileges and immunities usually make enforcement in court difficult.

[6] While Article 48 refers to a 'public authority or body', the Regulation does not define what constitutes a 'public authority or body'. In line with Recital 65 of the Regulation, the EDPS considers that this notion covers both public bodies in third countries and international organisations. This interpretation is also based on the draft Guidelines of the European Data Protection Board (the EDPB) on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 (the GDPR) for transfers of personal data between EEA and non-EEA public authorities and bodies.

[7] The network of EUIs' DPOs is working on a set of "template" clauses for this purpose.

Once such an arrangement can be agreed between X and A, X should send it to the EDPS for consultation and authorisation under Article 48(3)(b) of the Regulation[8]. Subject to the EDPS authorisation, the transfers of personal data to A for the processing can then lawfully take place based on those clauses.

We hope this information was useful. Should you have any doubts, please do not hesitate to contact us.

Yours sincerely,

Wojciech Rafał WIEWIÓROWSKI

[8] Please see some previous authorisations/cases that could help X in their process of elaborating an administrative arrangement:
ESMA case: https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/iosco-esma-administrative_en;
Some background information on ESMA case, see EDPB Opinion: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-42019-draft-administrative-arrangement_en,
and text of the arrangement: https://edpb.europa.eu/our-work-tools/our-documents/other/draft-administrative-arrangement-transfer-personal-data-between_en