EDPS OPINION ON THE LEGAL BASIS FOR PERSONAL DATA TRANSFERS TO THE EUROPEAN UNIVERSITY INSTITUTE (Case 2020-0880)

1. INTRODUCTION

- This Opinion relates to the European Court of Auditors ('the Court of Auditors') consultation on the legal basis for personal data transfers to the European University Institute.

- The EDPS issues this Opinion in accordance with Articles 57(1)(g) and 58(3)(c) of Regulation (EU) 2018/1725[1] ('the Regulation').

2. FACTUAL DESCRIPTION

The Court of Auditors would like to sign a contract with the European University Institute on providing trainings. The DPO of the Court of Auditors asked the EDPS on the applicable legal basis and possible data protection guarantees for the data subjects and the parties of such contract.

3. LEGAL ANALYSIS

a) Controller - processor or joint controllers' relationship

In the request for consultation, the DPO mentioned that the Court of Auditors and the European University Institute would be joint controllers in accordance to a draft contract on providing training. However in the further explanations provided, it was clarified that the trainings would be organised by the European University Institute, while the Court of Auditors would decide which staff members will take part in the trainings and which trainings are of interests for the Court. This suggests that the Court of Auditors would actually independently determine the purpose and means of processing personal data of its staff members. Therefore the EDPS encourages the Court of Auditors to carefully check the possible role of the controller and processor between both parties.

If in fact this is rather a controller - processor relationship, this has to be properly reflected in a contract or other legal act under Union or Member State law binding on the parties. In light

[1] Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.

of Article 29[2] of the Regulation, the Court of Auditors being the controller, should ensure that the contract (or other legal act) with the European University Institute contains clear and precise obligations, roles and tasks of the respective parties regarding data protection as well as all the requirements provided in Article 29(3) of the Regulation.

On the other hand, if this is a joint controllers' relationship then the Court of Auditors and the European University Institute need to clearly identify and define their respective responsibilities with regard to their specific obligations under Regulation. To this end they have to enter into a specific arrangement, the essence of which shall be made available to the data subjects as provided in Article 28 of the Regulation.

b) Transfer of personal data to an international organisation

The European University Institute is an international organisation established by the Convention setting up the European University Institute[3] signed by the EU Member States. As an international organisation, the European University Institute does not apply directly the European data protection legal framework, but applies the internal regulation - the President decision No. 10/2019 of 18 February 2019[4], which is drafted in accordance with the principles contained in the Convention establishing the European University Institute, signed on 19 April 1972, and with the Protocol on Privileges and Immunities annexed to it.

The cooperation on providing training between the Court of Auditors and the European University Institute entails that some personal data would need to be transferred from a European institution to an international organisation.

Chapter V of the Regulation provides for specific mechanisms and conditions to allow transfers of personal data by EU institutions and bodies, to a third country or an international organisation. These mechanisms and conditions aim to ensure that the level of protection of natural persons guaranteed by the EU data protection legislation is not undermined.

The first mechanism is the adoption by the EU Commission of an adequacy decision recognizing that the third country or an international organisation provides a standard with regard to data protection that is essentially equivalent to that within the EU.[5] However, until now the EU Commission has not adopted any adequacy decision concerning international organisations.

In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards and on the condition that enforceable rights and effective legal remedies are available for individuals[6]. A legally binding and enforceable instrument between public authorities or bodies may provide for such appropriate safeguards.[7] Such safeguards may also be provided, subject to the authorisation from the EDPS, by inserting provisions into

[2] See EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 (the EDPS Guidelines)
[3] Convention setting up the European University Institute: https://www.eui.eu/Documents/AboutEUI/Convention/Consolidated-Convention-following-UK-exit.pdf
[4] President decision No 10/2019: https://www.eui.eu/Documents/AboutEUI/Organization/DataProtection/PresDecision10-2019-DataProtection.pdf
[5] Article 47 of the Regulation.
[6] Article 48(1) of the Regulation.
[7] Article 48 (2) (a) of the Regulation.

administrative arrangements between public authorities of bodies which include enforceable and effective data subject rights.[8]

If a transfer of personal data is envisaged to a third country or an international organisation that is not the subject of an adequacy decision and if appropriate safeguards are absent, a transfer can be made based on a number of derogations for specific situations[9]. However, data exporters should first endeavour possibilities to frame the transfer with one of the mechanisms providing appropriate safeguards.[10] Moreover, the EU institution must inform the EDPS of the categories of cases in which derogations have been applied.[11]

For recurring and structural exchanges of personal data with public authorities, as in the case of the envisaged model, the EDPS considers that binding international agreements[12] or administrative arrangements are the relevant transfer instruments to be used[13].

A list of minimum safeguards can be found in the European Data Protection Board (EDPB) - guidelines adopted on 18 January 2020 on Articles 46(2)(a) and 46(3)(b) of the GDPR[14] for transfers of personal data between EEA and non-EEA public authorities and bodies.[15] It must be noted, however, that these guidelines are currently under the EDPB review to properly reflect the Schrems II judgement[16] of the Court of Justice of the European Union. The EDPS has also adopted a decision[17] on the safeguards to be included in an administrative arrangement for transfers of personal data between an EU agency and an international organisation pursuant to Article 48(3)(b) of the Regulation. Please also note that the DPOs network is currently working on a draft model administrative arrangement.

Based on the above-mentioned EDPB guidelines and the EDPS decision, the administrative arrangement between the Court of Auditors and the European University Institute should include the following guarantees:

- **Definitions of key concepts and rights** of the European data protection legal framework such as personal data, onward transfers, sharing of personal data, personal data breach, processing, professional secrecy, profiling, data subjects rights mentioning right of access, right of rectification, right of erasure, right of information, right of objection, right of restriction of processing, which are in line with the definitions contained in the Regulation.
- **Principle of purpose limitation and prohibition of any further use**: a receiving party should process data only for the purpose data were exchanged and any further processing incompatible with the initial purpose of the exchange of data should be prohibited.
- **Principle of data quality and proportionality**: a transferring party should only transfer accurate and up to date personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed. Each party

---

8 Article 48 (3) (b) of the Regulation.
9 Article 50 of the Regulation.
10 Derogations should not allow recurrent, massive and structural transfers (See by analogy Recital 72 of GDPR on transfers based on derogations).
11 Article 48(6) of the Regulation.
12 Article 48 (2) (a) of the Regulation.
13 Article 48(3)(b) of the Regulation.
14 These provisions correspond to Article 48(2)(a) and 48(3)(b) of the Regulation.
15 EDPB guidelines 02/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (the 'EDPB guidelines').
16 Case C-311/18.
17 EDPS Decision of 13 March 2019 concerning the use of the IOSCO-ESMA Administrative Arrangement by the European Securities and Markets Authority (the 'EDPS decision').

should inform the other if it becomes aware that transferred personal data is incorrect. Having regard to the purposes for which the personal data have been transferred and further processed, each party should supplement, erase, block, correct or otherwise rectify the personal data, as appropriate.

- **Principle of transparency**: a general notice to data subjects should be provided in relation to the processing carried out, including the transfer, the type of entities to which data may be transferred, the rights available to them under the applicable legal requirements, including how to exercise those rights and information about any applicable restrictions on the exercise of such right, available redress mechanisms and the contact details for submitting a dispute or claim. The administrative arrangement should explain how this notice should be provided to data subjects and if individual notice needs to be provided.
- **Principle of data retention**: personal data should be retained for no longer than is necessary for the purpose for which the data are processed in compliance with the applicable laws, rules and/or regulation governing the retention of such data.
- **Security and confidentiality measures:** appropriate administrative, technical and physical security measures should be taken, including for example, marking information as personal data, restricting who has access to personal data, providing secure storage of personal data, or implementing policies designed to ensure personal data are kept secure and confidential. The arrangement should also provide for procedures for cases of personal data breaches and set out that if a receiving party becomes aware of a personal data breach, it informs a transferring party as soon as possible and use reasonable and appropriate means to remedy the personal data breach and minimize the potential adverse effects.
- **Safeguards relating to data subject rights**: data subjects should be able to obtain confirmation of whether their data have been transferred. Data subjects should also be provided with access to their personal data upon request. In addition, data subjects may request that their data are rectified, erased, blocked or restricted and where relevant the right to oppose to the data processing on grounds relating to his or her particular situation. Any restriction to these rights has to be provided by law and is allowed only to the extent and for as long as this is necessary to protect confidentiality pursuant to professional secrecy or other legal obligations.
- **Restrictions on onward transfers**: Onward transfers to a third party in another country who is not covered by an adequacy decision adopted by the European Commission can only take place with the prior written consent of a transferring party, and if the third party provides appropriate assurances that are consistent with the safeguards in the administrative arrangement.
- **Redress**: data subjects should have the right to obtain redress and, where appropriate, to receive compensation. The administrative arrangement should provide for alternative dispute settlement mechanisms in case judicial remedies are not available for an international organisation signing the arrangement. Other, alternative methods may be mediation or dispute resolution proceedings. There should also be provisions allowing for suspension of data transfers in case a transferring party believes that a receiving party has not acted in relation to claims or disputes in line with the safeguards set out in the working arrangement. The administrative arrangement should provide that parties inform each other about disputes or claims related to the arrangement and should use their best efforts to settle them amicably in a timely manner. Redress mechanisms should also be available for alleged data breaches. Situations where an international organisation is unable to implement the safeguards of the arrangement should also be covered. In such cases the European Union Institution should be informed without delay and transfers should be suspended until the safeguards of the arrangement can be implemented.

- **Oversight mechanism** should consist of a combination of periodic reviews conducted externally and internally by each party. The combination of the external and internal oversight as well as the adopted possible consequences following a negative review–which may include a recommendation to suspend participation in the administrative arrangements – provides for a satisfactory level of protection. The EDPS also recommends that the administrative arrangement include the voluntary commitment of the receiving party to cooperate with the EDPS as supervisory authority of the Court of Auditors. In case this is not possible, independent oversight could be guaranteed through functionally autonomous mechanisms. The latter must be a body that, while not external itself, carries out its functions independently, i.e. free from instructions, with sufficient human, technical and financial resources.

Taking into account that the European University Institute President decision No 10/2019 regarding data protection[18] is based to a large extent on the European data protection legal framework, it seems that most of the guarantees listed above (data protection principles, security, data subjects rights, some definitions of key concepts) are already provided there. However other safeguards need to be further elaborated, especially those concerning restrictions on onward transfers, redress (including further clarification on the judicial redress by the Organ of First Instance) and oversight mechanism.

4. CONCLUSION

In light of the above, the EDPS recommends that the Court of Auditors and the European University Institute clarify the respective roles of both parties as regard to processing of personal data and draft the appropriate administrative arrangement taking into account the guarantees explained in this letter. In accordance to Article 48 (3) of the Regulation the administrative arrangement requires an authorisation by the EDPS.

Brussels, 12 November 2020

Wojciech Rafał WIEWIÓROWSKI
(*e-signed*)

[18]President decision No 10/2019:
https://www.eui.eu/Documents/AboutEUI/Organization/DataProtection/PresDecision10-2019-DataProtection.pdf