EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

To the heads of all Union institutions,
bodies and agencies

Brussels, 2nd October 2020

[redacted] D(2020) 2169 **C 2020-0766**
Please use edps@edps.europa.eu
for all correspondence

Subject: Order of the EDPS pursuant to Article 58(1)(a) of Regulation (EU) 2018/1725 to provide information

Dear Sir or Madam,

On 16 July, the Court of Justice of the EU issued the Judgment in case **C-311/18**, known as 'Schrems II' (the 'Judgment'), concerning Commission Decision 2010/87/EC on Standard Contractual Clauses ('SCCs') for transfers to third countries in general and the level of protection ensured in the United States in particular (Privacy Shield[1]). As this Judgment has serious implications on personal data transfers carried out by Union institutions, bodies, offices and agencies ('EUIs'), I address this letter to you in order to inform you about the information I expect your institution to provide.

I. Background information

The Court in its Judgment notably ruled the following:

- The Privacy Shield is invalidated in particular on the basis of (i) the lack of proportionality caused by mass surveillance programmes based on Section 702 of the FISA[2] and E.O.[3] 12333 read in conjunction with PPD-28 and (ii) the lack of effective remedies in the US essentially equivalent to those required by Article 47 of the Charter.
- The validity of the 2010 Standard Contractual Clauses ('SCCs') for transfers is confirmed (Commission Decision 2010/87/EC). However, that validity, depends on whether the SCCs include effective mechanisms to ensure compliance in practice with the level of protection essentially equivalent to that guaranteed within the EU by the General Data Protection Regulation ('GDPR')[4] and the transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or in case it is impossible to honour them.

1 Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
2 Foreign Intelligence Surveillance Act
3 Executive Order.
4 This is to be understood as a reference to the similar provisions of Regulation (EU) 2018/1725 for the EUIs.

- The SCCs for transfers may then require, depending on the prevailing position in a particular third country, the adoption of 'supplementary measures' by the controller in order to ensure compliance with the level of protection guaranteed within the EU.
- Commission Decision 2010/87/EC imposes an obligation on the data exporter (controller) and the recipient of the data (the 'data importer') to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether that level of protection is respected in the third country concerned. The Commission Decision 2010/87/EC further requires the data importer to inform the data exporter of any inability to comply with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clauses, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer. However, if the controller intends to keep transferring data despite this conclusion, it must notify their competent supervisory authority.
- The competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

The Judgement has far-reaching consequences as the threshold set by the Court is meant to apply to all appropriate safeguards provided by controllers or processors under Article 46 GDPR[5] in order to transfer data from the European Economic Area (EEA) to any third country.

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 56 of Regulation (EU) 2018/1725 ('the Regulation')[6]. It is the duty of the EDPS under Article 57(1)(a) and (f) of the Regulation to monitor and ensure the application of the Regulation with regard to the processing of personal data by any EUI, including through the use of its corrective powers pursuant to Article 58(2) of the Regulation.

Therefore, pursuant to Article 58(1)a of the Regulation, I ask you to provide information concerning on-going processing operations and contracts involving transfers to third countries (II)while paying special attention to new processing operations and contracts that would involve such transfers (III).

II. Information required from your EUI concerning on-going processing operations and on-going contracts involving transfers to third countries

In this respect, I ask you to provide the following information:

1. **Mapping exercise** (to be concluded by 31 October 2020)

In order to enable the EDPS to fulfil its tasks under Article 57 of the Regulation and for the EUIs to comply with the present order and the Regulation, it is necessary that EUIs carry out a mapping of data flows.

---

[5] This is to be understood as a reference to Article 48 of Regulation (EU) 2018/1725 for the EUIs.

[6] Regulation (EU) 2018/1725 of the European Parliament and of 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, p. 39.

In this respect, I would like to ask you to **launch immediately**[7] **a mapping exercise** with the aim to map data transfers (including onward transfers) for on-going contracts and procurement procedures and other types of cooperation in the context of which personal data is transferred. The mapping exercise is to list in particular:

- each processing activity for which data is transferred to / accessed from a third country (including purposes and means of processing);
- destinations of data transfers (including those of all processors and sub-processors);
- type of recipient (data importer);
- transfer tool used (of the ones provided in Chapter V of the Regulation);
- types of personal data transferred;
- categories of data subjects affected;
- any onward transfers (including to which countries and which recipients, transfer tool used, types of personal data and categories of data subjects affected).

Your records of processing activities (Article 31 of the Regulation) are a good starting point for this task. You should also check the contracts you have with processors and with other controllers, as well as other arrangements you might have in the context of which personal data is transferred. In line with Article 31(2) of the Regulation, each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing inter alia information on international transfers of personal data. At the end of this task, you should be able to locate where exactly the personal data you exported may be. Note that remote access (e.g. in support situations) is also considered a transfer.

2. **Report to the EDPS any identified risks and gaps based on the mapping exercise** (at the latest by 15 November 2020). The following cases should be reported to the EDPS:
    1) Transfers which are not based on any transfer tool (e.g.: onward transfers between the EUI's processor and a sub-processor that are not framed by any standard or *ad hoc* contractual clauses or another arrangement);
    2) Transfers that are based on a derogation under Article 50 of the Regulation;
    3) 'High-risk transfers' to the US in light of the Judgment. Those "high-risk transfers" concern any transfer to entities clearly subject to Section 702 FISA or E.O. 12333[8] ***and*** involving:
        - large scale processing operations[9]; *or*
        - complex processing operations or sets of operations[10]; *or*
        - processing of sensitive data or data of a highly personal nature[11].

---

[7] We strongly recommend launching the exercise without delay as the input of the data importers (processors/sub-processors) is likely to be required in order to complete the exercise.

[8] Section 702 FISA applies to all "electronic communication service provider" (see the definition under 50 USC § 1881(b)(4)), while EO 12 333 organises electronic surveillance, which is defined as the "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter" (3.4; b)).

[9] See EDPS reply to informal consultation on the application of Article 39(3)(b) of Regulation (EU) 2018/1725. See also Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01, adopted by the Article 29 Working Party and endorsed by the EDPB.

[10] For example processing operations involving large datasets of complex data structure, linking different databases, big data analytics, the use of novel technologies or complex techniques (like those in profiling and automated-decision making processes), or involving many different or unknown actors.

[11] See Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01, adopted by the Article 29 Working Party and endorsed by the EDPB, pages 9-10: "*4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about*

The report should mention the risks under case 3) and explain all mitigating measures taken to address those risks. These reports should provide sufficient information for the EDPS to understand the transfers mentioned under the cases 1) to 3) above, as well as the risks and what measures, if any, the EUIs had put in place. In particular, all the information requested for the mapping exercise under point 1 in relation to the particular processing activity and transfer concerned should be included.

Your EUI should require the help of processors and/or other data importers to identify transfers (including onward ones) and destinations for personal data processed on behalf of the EUI. While your DPO is to be closely associated in dissemination of information to controllers and later in gathering and synthesising information in the report to the EDPS, the primary responsibility lies with the controllers of the data processing within your EUI.

3. **Further steps**

The abovementioned mapping exercise will help EUIs to carry out, **in a second phase,** case-by-case "transfer impact assessments" ('TIA') with the aim to identify whether an essentially equivalent level of protection as provided in the EU/EEA is afforded in the third country of destination. The factual description of the circumstances of each transfer should be based on the mapping exercise done by data exporter and should include additional information provided by data importer. Identification and implementation of 'supplementary measures' or 'additional safeguards' may be necessary in order to ensure such equivalence in the level of protection[12]. The circumstances of the transfer will also influence the identification of any appropriate supplementary measures.

Concluding this second phase, EUIs should reach a decision as to whether it is possible to continue the transfers identified in the mapping exercise (with appropriate safeguards and supplementary measures or based on a derogation).

With the aim to facilitate TIAs, the EDPS will provide EUIs in due time with guidance on the elements that they should take into account when conducting such assessments, as well as with guidance on supplementary measures. Possible further guidance issued in the meantime by the European Data Protection Board will be taken into account[13].

Let me recall that in line with Article 46 of the Regulation, any transfer of personal data to a third country or international organisation shall take place only if, subject to the other provisions of the Regulation, the conditions laid down in Chapter V are complied with, including for

---

individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications."

[12] See paragraph 133 of the Judgment and recital 66 of the Regulation.

[13] Please note that a first set of FAQs was adopted by the EDPB on 23 July 2020. See also the statements of the EDPS and the EDPB following the Schrems II judgement.

onward transfers. I wish furthermore to underline the limited use of derogations pursuant to Article 50 of the Regulation[14]. The EDPS in its supervisory activities will put special attention to control if derogations are used properly.

III. New processing operations and new contracts that will entail transfers of personal data

The EDPS' own-initiative investigation into the use of Microsoft products and services by EUIs and our recommendations to the EUIs in that regard confirm the importance of ensuring a level of protection essentially equivalent to that guaranteed within the EU by EU data protection laws, read in light of the Charter. The EDPS already flagged in this context a number of linked issues concerning sub-processors, data location, international transfers and the risk of unlawful disclosure of data – issues that the EUIs were unable to control and ensure proper safeguards to protect data that left the EU/EEA. The issues we raised in our investigation report are consistent with concerns of the Court in its Judgment, which we are assessing in relation to any processors of the EUIs.

In light of the above and following the Judgment, , the EDPS is convinced that EUIs need a strong precautionary approach as regards the use of any service provider and any new processing operations. For this reason, the EDPS strongly encourages that EUIs ensure that any new processing operations or new contracts with any service providers, involve no transfers of personal data to the U.S. In this regard, please note that any enforcement actions by the EDPS to ensure compliance with the Regulation will also cover future activities of EUIs, not only those that took place before the receipt of this letter.

As a community of EUIs, we believe it is our common duty to protect the rights of individuals and safeguard their personal data, including when transferred to third countries, stemming from the Charter of Fundamental Rights, the Regulation and the jurisprudence of the Court of Justice of the European Union. Your cooperation in applying the Court's Judgment is therefore of utmost importance.

Yours sincerely,

[**E-signed**]

Wojciech Rafał WIEWIÓROWSKI

cc: Data Protection Officer of your institution

[14] In this respect, see also the EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.