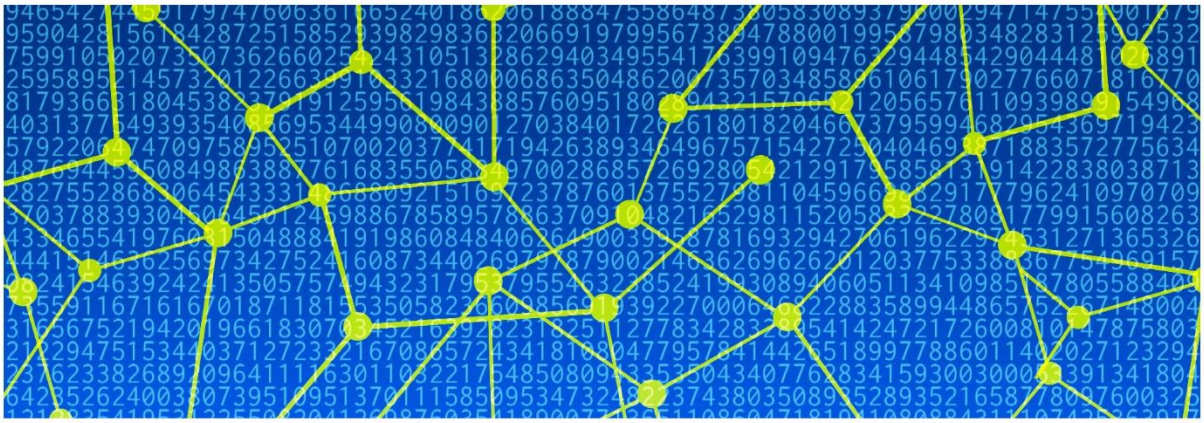

EUROPEAN DATA PROTECTION SUPERVISOR

Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling

EDPS

29 October 2020

Executive Summary

The EDPS has issued this Strategy, following the Court of Justice of the European Union's judgement in case C-311/18, known as '**Schrems II'** (the 'Judgment'). The Judgement concerns the European Commission's Decision 2010/87/EC on Standard Contractual Clauses ('SCCs') for transfers to third countries, and in particular, the level of protection ensured in the United States (Privacy Shield).

The present **strategy aims to ensure and monitor compliance of European Union Institutions', bodies, offices and agencies (EUIs) with the Judgement. The document addresses both short and medium term actions for EUIs and the EDPS.** The goal is to ensure that **ongoing and future** international transfers comply with the EU Charter of Fundamental Rights as well as applicable EU data protection legislation, specifically Chapter V of Regulation (EU) 2018/1725 ('the Regulation'), as interpreted in the Judgement. The strategy builds on the **cooperation** and **accountability** of controllers to ensure this compliance and that the essentially equivalent level of protection applied in the EU is guaranteed when EUIs transfer personal data outside of the EEA.

The EDPS identified as **priority criteria** transfers **carried out by EUIs or on their behalf in the context of controller to processor contracts and/or processor to sub-processor contracts, particularly towards the United States**. **An action plan** was developed to streamline compliance and enforcement measures, by distinguishing between **short-term and medium-term compliance actions.**

As a short-term compliance action, the EDPS issued an **order to EUIs**, on 5 October 2020, for them to **complete a mapping exercise** identifying which on-going contracts, procurement procedures and other types of cooperation involve transfers of data. EUIs are expected to **report to the EDPS** on certain types of transfers. These are transfers that do not have a legal basis, transfers that are based on derogations and transfers to private entities towards the U.S. presenting high risks for data subjects. With regard to **new processing operations** or new contracts with service providers, the **EDPS strongly encourages** EUIs to **avoid** processing activities that involve **transfers of personal data to the United States.**

As a **medium-term** compliance action, the EDPS will provide **guidance** and pursue compliance and/or enforcement actions for transfers towards the U.S. or other third countries on a case-by-case basis. EUIs will be asked to carry out case-by-case **Transfer Impact Assessments** (TIAs) to identify for the specific transfer at stake whether an essentially equivalent level of protection, as provided in the EU/EEA, is afforded in the third country of destination. Based on these assessments that are to be carried out with the help of data importers, EUIs should reach a decision as to whether it is possible to continue the transfers identified in the mapping exercise. EUIs will be asked to **report to the EDPS** on the use of derogations, on transfers that are continued towards a third country that do not have an essentially equivalent level of protection, and on transfers that are suspended or terminated because of the absence of an essentially equivalent level of protection in the country of destination. We will also start exploring the possibility of **joint assessments** of the level of protection of personal data afforded in third countries in order to provide guidance to controllers.

The **EDPS will continue to cooperate closely with other Data Protection Authorities (DPAs) within the European Data Protection Board** (EDPB) to ensure the Judgement's consistent implementation in the EEA.

TABLE OF CONTENTS

1. BACKGROUND

On 16 July, the Court of Justice of the EU issued its Judgment regarding case **C-311/18**, known as 'Schrems II' (the 'Judgment')[1], which concerned the European Commission's Decision 2010/87/EC[2] on Standard Contractual Clauses ('SCCs') for transfers of data to third countries and the level of data protection ensured in the United States (Privacy Shield)[3].

In its Judgment, the Court clarified **the roles and responsibilities** of controllers, recipients of data outside of the European Economic Area (EEA) (data importers) and supervisory authorities. To this end, the Court ruled the following:

- The Court invalidated the Privacy Shield adequacy Decision and confirmed that the SCCs were valid providing that they include effective mechanisms to ensure compliance in practice with the *"essentially equivalent"* level of protection guaranteed within the EU by the General Data Protection Regulation[4] (GDPR).[5] Transfers of personal data pursuant to the SCCs are suspended or prohibited in the event of a breach of such clauses, or in case it is impossible to honour them.
- The SCCs for transfers may then require, depending on the prevailing position of 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.
- In order to continue these data transfers, the Court stresses that before transferring personal data to a third country, it is the data exporters' and data importers' responsibility to assess whether the legislation of the third country of destination enables the data importer to comply with the guarantees provided through the transfer tools in place. If this is not the case, it is also the exporter and the importer's duty to assess whether they can implement supplementary measures to ensure an essentially equivalent level of protection as provided by EU law. Should data exporters, after taking into account the circumstances of the transfer and possible supplementary measures, conclude that appropriate safeguards cannot be ensured, they are required to suspend or terminate the transfer of personal data. In case the exporter intends nevertheless to continue the transfer of personal data, they must notify their competent SA[6].
- The competent supervisory authority is required to suspend or prohibit a transfer of personal data to a third country pursuant to the SCCs if, when considering the circumstances of that transfer, those clauses are not or cannot be complied with in the third country of destination and the protection of the data transferred under EU law cannot be ensured by other means.

2. OBJECTIVES

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 56 of the Regulation (EU) 2018/1725[7] ('the Regulation'). 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 Union institutions, bodies, offices and agencies ('EUIs'), including by using its investigative and corrective powers pursuant to Article 58(1) and 58(2) of the Regulation.

The EDPS has therefore developed **a strategy to ensure and monitor compliance of EUIs with the Judgement**. This present document addresses both **short and medium term actions for EUIs and the EDPS.** The goal is to make sure that **ongoing and future** international transfers comply with Articles 7, 8 and 47 of the EU Charter of Fundamental Rights as well as applicable EU data protection legislation, in particular Chapter V of the Regulation, as interpreted in the Judgement.

In compliance with the Judgement, this strategy builds on the **accountability and cooperation** of EUIs as the fundamental elements necessary for its success. According to the principle of accountability[8], controllers shall ensure, verify and demonstrate compliance with the Regulation, including with the provisions on transfers of personal data. EUIs shall remain in control and take informed decisions when they select processors and allow transfers of personal data outside the EEA. The objective of the Regulation is to ensure the protection of fundamental rights and freedoms of individuals, in particular their right to the protection of personal data, and to ensure continuity of this protection in case of transfers of personal data[9]. As laid down in Article 46, any transfer must not only comply with Chapter V but is also subject to other provisions of the Regulation. The use of transfer tools available under Chapter V and the available derogations should not undermine the level of protection of personal data guaranteed by the Regulation[10]. This was also clearly confirmed by the Court when it reaffirmed the **obligation for controllers to verify, before the transfer takes place, whether an essentially equivalent level of protection is ensured in practice, in the country of destination and to suspend or terminate transfers if such a level of protection cannot be guaranteed.** Besides, according to the principle of cooperation[11], **EUIs shall cooperate, on request, with the EDPS in the performance of his tasks**. The EDPS expects EUIs to cooperate at the highest level, as it is of utmost importance to apply the Court's Judgment.

To ensure compliance with the Regulation regarding all international transfers, the EDPS identified the following **priority criteria** (see point 3.) and developed an **action plan** (see point 4.) to streamline compliance and enforcement actions. Furthermore, **cooperation with the EDPB,** as explained in the present document (see point 5.), will ensure the consistent implementation of the Judgement throughout the EEA.

The present strategy is without prejudice to the **handling and investigating of complaints** received by the EDPS on this topic.

3. PRIORITY CRITERIA

The Judgement has far-reaching consequences as the threshold set by the Court applies to all appropriate safeguards under Article 46 of the GDPR[12] as the legal tools used to transfer data from the EEA to any third country, including transfers between public authorities. However, it appears from recent consultations with EUIs and investigations conducted by the EDPS[13] that **a prominent part of personal data transfers by EUIs or on their behalf concern data flows carried out in the context of contractual relationships between controllers and processors and/or processors and sub-processors, particularly towards the United States.**

The EDPS' report on the 2017 survey entitled, *Measuring compliance with data protection rules in EU institutions*, provides evidence that there has been a significant rise[14] in the number

of transfers related to the core business of EUIs[15] in recent years. This number is even higher now, due to the increased use of ICT services and social media. The EDPS' own-initiative investigation into the use of Microsoft products and services by EUIs[16] and subsequent recommendations in that regard confirms the importance to ensure a level of protection that is essentially equivalent as the one guaranteed within the EU, as provided by relevant data protection laws, to be interpreted in accordance with the EU Charter. In this context, the EDPS has already flagged 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 the concerns expressed in the Court's Judgment, which we are assessing in relation to any processor agreed to by EUIs.

Moreover, a majority of data flows to processors most probably happen because EUIs use service providers that are either based in the U.S. or that use sub-processors based in the U.S., in particular for ICT services, which fall under the scope of U.S. surveillance laws. Such companies have primarily relied on the Privacy Shield adequacy Decision to transfer personal data to the U.S. and the use of SCCs as a secondary measure.

Therefore, the present Strategy **emphasises the priority to address transfers of data by EUIs or on their behalf in the context of controller to processor contract and/or processor to sub-processor contracts, in particular towards the United States.**

4. ACTION PLAN FOR BRINGING EUIs INTO COMPLIANCE

The EDPS considers a **twofold approach** as the most appropriate: (1) Identify urgent **compliance and/or enforcement actions** through a risk based approach for transfers towards the U.S. presenting high risks for data subjects and in parallel (2) provide **guidance** and pursue mid-term case-by-case EDPS compliance and or enforcement actions for all transfers towards the U.S. or other third countries.

The EDPS Strategy for EUIs to ensure and monitor compliance with the Judgement is essentially divided in two phases, with short and mid-term actions.

4.1. Short term - Mapping exercise and immediate compliance priorities

Mapping

On 5 October 2020, the EDPS issued an **order to EUIs** to carry out an inventory of all **on-going processing operations and contracts** involving transfers to third countries. Institutions are requested to **complete a mapping exercise** by the end of October to identify data transfers for on-going contracts, procurement procedures and other types of cooperation. EUIs' inventory should describe the processing operations, destinations, recipients, transfer tools used, types of personal data transferred, categories of data subjects affected, as well as information on onward transfers.

Taking into account the priority criteria (transfers towards private entities, particularly towards the U.S.) set out in the Strategy, **the EDPS has developed a risk based approach, with benchmarks for short term compliance** and **reinforced monitoring of the (improper) use of derogations.**

The risk-based approach aims to identify priority enforcement actions where no essentially equivalent level of protection for transfers would be guaranteed, focusing in particular on transfers towards processors and onward transfers to sub-processors that are private entities, particularly towards the U.S.

Reporting

EUIs are expected to **report to the EDPS by 15 November 2020** at the latest, on specific risks and gaps they identified during this mapping exercise. Furthermore, they have to provide specific and transparent information to the EDPS on three main categories of transfers, which are likely to present higher risks for the rights and freedoms of individuals and are identified by the EDPS as supervision priorities before the end of 2020:

a) illegal transfers which are not based on any transfer tool[17];

b) transfers that are based on a derogation under Article 50 of the Regulation; and

c) 'high-risk transfers' to the U.S. to entities clearly subject to Section 702 FISA[18] or E.O. 12333[19], **and** involving either large scale processing operations[20] or complex processing operations[21] or processing of sensitive data or data of a highly personal nature.[22]

Based on this first reporting exercise, the EDPS may take **enforcement actions to bring those transfers into compliance with the Regulation or to suspend those transfers, where appropriate**.

Caution for future services and new processing operations

With regard to the use of any new service providers and **new processing operations** carried out with appropriate safeguards and appropriate supplementary measures, the EDPS has requested EUIs to take a **strong precautionary approach**. The **EDPS strongly encourages** EUIs to ensure that any **new processing operations** or new contracts with any service providers does not involve **transfers of personal data to the United States.**

4.2. Medium Term - Guidance and Transfer Impact Assessments

Transfer Impact Assessments (TIAs)

EUIs will be asked to carry out case-by-case **Transfer Impact Assessments** (TIAs) to identify whether an essentially equivalent level of protection as provided in the EU/EEA is afforded in the third country of destination.

Following the expected EDPB guidance on appropriate supplementary measures, **the EDPS will provide a list of preliminary questions for EUI controllers** to launch TIAs with data importers.

Based on these assessments carried out with the help of data importers, EUIs should reach a decision as to whether it is possible to continue transfers identified in the mapping exercise. To be able to continue with these transfers, EUIs, together with data importers, may need to identify and implement **supplementary measures** or additional safeguards to ensure an essentially equivalent level of protection as provided in the EEA. EUIs shall also assess whether one of the **derogations** of Article 50 of the Regulation could apply in their specific situation, providing that the conditions set forth in that Article are fulfilled.

Reporting

Depending on the outcome of the TIAs, EUIs will be asked to **report to the EDPS in the course of spring 2021** on the following three categories of transfers:

a) Transfers to a third country that do not ensure an essentially equivalent level of protection;

b) Transfers that are suspended or terminated shall be notified in line with Article 47(2) of the Regulation if the EUI considers that the third country does not ensure an essentially equivalent level of protection;

c) For transfers based on derogations, categories of cases in which Article 50 has been applied shall be notified in line with Article 50(6) of the Regulation.

Based on the outcome of the mapping exercise combined with the conclusions drawn from TIAs, and in cooperation with the EDPB, the EDPS will establish long-term compliance priorities for 2021 which will be communicated in a timely and appropriate manner.

Joint assessments

The EDPS will also start exploring the possibility of **joint assessments** of the level of protection of personal data afforded in third countries and how these could be coordinated between authorities, controllers and other stakeholders to provide guidance and ensure compliance with the Judgement.

5. COOPERATION WITH THE EDPB

Within the EDPB, **the EDPS is working with the other DPAs in the EEA on developing further guidance and recommendations to assist controllers and processors** in their duties to identify and implement appropriate supplementary measures to ensure an adequate level of protection when transferring data to third countries.

This compliance strategy will closely follow the guidance of the EDPB and will be adjusted, where necessary, to ensure a consistent interpretation and implementation of the Judgement by EUIs and throughout the EEA.

[1] Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

[2] 2010/87/EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) OJ L 39, 12.2.2010,
[3] Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1. This is to be understood as a reference to the similar provisions of Regulation (EU) 2018/1725.
[5] This is to be understood as a reference to the similar provisions of Regulation (EU) 2018/1725 for the EUIs.
[6] See in particular recital 145 of the Court's judgment, and Clause 4(g) Commission decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) of Commission Decision 2004/915/EC.
[7] Regulation (EU) 2018/1725 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.
[8] Article 26 of Regulation 2018/1725
[9] Article 1(2) of Regulation 2018/1725
[10] Article 46 of Regulation 2018/1725
[11] Article 32 of Regulation 2018/1725
[12] This is to be understood as a reference to Article 48 of Regulation (EU) 2018/1725 for the EUIs.
[13] EDPS' own-initiative investigation into the use of Microsoft products and services by EUIs
[14] The number of EUIs reporting transfers had almost doubled to 30 EUIs out of 64.
[15] Where the EUIs carry out tasks in the public interest entrusted to them by EU law.
[16] see footnote n. 11
[17] For example 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.
[18] Foreign Intelligence Surveillance Act
[19] Executive Order
[20] 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.
[21] 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.
[22] 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 (point4)