CHIOMENTI

Key News

IP, TMT and Data Protection Department
December 2020

Summary

Definitions

CGUE	Court of Justice of the European Union
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
GDPR	Regulation (EU) 2016/679
EEA	European Economic Area
Swedish DPA	Swedish Data Protection Authority - *Datainspektionen*

Personal data transfer after the schrems II ruling: some preliminary remarks

With the ruling of July 16, 2020 in the Schrems II case (Case C-311/18) - previously discussed in detail here - the CJEU has returned to the issue of transfers of personal data to third countries, declaring the invalidity of the "Privacy Shield EU-US" (established by EU Implementing Decision 2016/1250 of the European Commission). The CJUE held that the

Privacy Shield EU-US does not ensure US compliance with the principle enshrined by the GDPR that requires for an adequate level of protection for the transfer of personal data outside the EEA. In particular, the decision is based on two grounds:

i. the predominance attributed by the U.S. legal system to the requirements of national security and the public interest over the fundamental rights of citizens, which justifies any interferences by the U.S. authorities in the context of public controls and surveillance programs of the intelligence services; and

ii. the lack of an adequate level of protection given to EU citizens concerned, who are not granted enforceable rights and effective remedies.

The above mentioned CJEU decision prohibited any transfer of personal data to the U.S. based on the Privacy Shield EU-US and also addressed the operation of the mechanism of the standard contractual clauses, making real the risk of legal uncertainty in assessing the adequacy of the level of protection in the light of GDPR, that is required for transfers of personal data to countries outside the European Economic Area.

Recently, the European Authorities have tried to provide a response with a series of initiatives illustrated below:

- the adoption of guidelines, recommendations and proposals aimed at providing operators intending to proceed with transfers outside the EEA of personal data with support in identifying and implementing the necessary additional actions and safeguards to be adopted (**see paragraphs I, II and III of this Newsletter**);

- the drafting of a new set of standard contractual clauses for transfers outside the EEA (**see paragraph IV of this Newsletter**).

While the resulting framework answers many of the questions that have arisen in the wake of the Schrems II decision, it indeed impose a burden on economic and institutional operators, who are called upon, in the fulfillment of their accountability, not only to implement a series of measures in relation to transfers outside the EEA, but also to carry out a proper assessment of the law or practice of the third country of reference.

Even the possible adoption of the new set of standard contractual clauses - which will be mandatory following the transitional period or, during the transitional period, outside of certain exempt circumstances (**see paragraph IV of this Newsletter**) - would not relieve operators of the obligation to conduct the aforementioned assessment. Rather, this set out a general framework of obligations and steps necessary to conduct the assessment, as well as to manage critical scenarios (e.g. requests from foreign law enforcement agencies or intelligence agencies).

In summary, prior to transfers outside the EEA, operators will need to ensure that the law or practice of the relevant third country does not jeopardize data protection safeguards and implement appropriate security measures. Secondly, in the course of the transfers, operators - as part of the accountability principle - will have to monitor on an ongoing basis the evolution of such laws and practices, as well as the adequacy of the implemented measures, in order to identify and manage potential detrimental changes in the level of protection of the personal data being transferred.

Being the first decision related to cross-border transfers of personal data after Schrems II ruling – although the latter was not "applicable" at times of events at stake – the one of the Swedish DPA is certainly noteworthy (**see paragraph V of this Newsletter**).

I EDPB RECOMMENDATIONS - MEASURES SUPPLEMENTING EXISTING TOOLS FOR CROSS-BORDER TRANSFERS OF PERSONAL DATA

On November 10, 2020, the EDPB adopted the "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" (the "**Recommendation**"), currently subject to public consultation.
With the Recommendation, the EDPB intends to shed light on the "additional safeguards" or "supplementary measures" to the transfer tools listed under Article 46.2 of GDPR, as referred to in the *Schrems II* ruling, that data exporters may adopt to ensure compliance with the level of protection required under EU law in a particular third country, by providing a methodology to determine whether and which additional measures shall be put in place for their transfers pursuant to the accountability principle underpinning the GDPR.

To this end, the Recommendation sets out a roadmap of the steps to be taken by data exporters (being them controllers or processors) to determine whether the adoption of any such supplementary measures is needed, consisting of the following six steps that are investigated and addressed more in detail in the text:

I. Step 1 – Identification of transfers: as a preliminary step to be adopted before any transfer is made, data exporters are advised to record and map all transfers (*e.g.* in the record of processing activities), including onwards transfers from a data importer located in a third country to another third country, as well as to verify compliance with information duties towards data subjects and with the data minimization principle. Significantly, the EDPB clarifies that remote access from a third country and/or storage in a cloud located outside the EAA shall also be regarded as a transfer.

II. Step 2 – Identification of transfer tools: following identification of the concerned transfers, data exporters must identify the relevant data transfer tools relied upon amongst those envisaged under Chapter V of GDPR (e.g., adequacy decisions, standard contractual clauses, binding corporate rules, derogations, etc.).

III. Step 3 – Assessment of the law of the third country: if a transfer is based upon any tools set forth by Article 46 of GDPR (including standard contractual clauses and binding corporate rules), data exporters must assess whether the law or practice of the third country may prevent the importer from complying with its obligations under the transfer tool relied upon. This assessment – which shall also consider the nature, scope and circumstances of the transfer – may be carried out with the collaboration of the importer, or also by referring to other sources of information which are listed non-exhaustively in Annex 3 to the Recommendation (*e.g.*, CJEU's case law, resolutions and reports from intergovernmental organizations, reports from academic institutions and NGOs, etc.).

IV. Step 4 – Adoption of supplementary measures: where the assessment above has revealed that the Article 46 GDPR transfer tool relied upon is not effective in the given case, data exporters must implement any supplementary measures that are necessary to ensure a level of protection of the data transferred in the third country which is essentially equivalent to that afforded by EU laws. Examples of possible supplementary measures, which shall be in any case identified on a case-by-case basis, are listed non-exhaustively in Annex 2 to the Recommendation, and include (i) technical measures; (ii) contractual measures; and (iii) organizational measures.

V. Step 5 – Procedural steps after identification of supplementary measures: depending on the Article 46 GDPR transfer tool relied upon, data exporters must put in place any formal procedural steps that may be required for the effective implementation of necessary protections.

VI. Step 6 – Re-evaluation at appropriate intervals: data exporters must monitor developments in the laws of the third country of destination on an ongoing basis (including, where appropriate, with the collaboration of data importers), so as to detect and address – in light of the accountability principle – potential detrimental changes in the level of personal data protection afforded by such third country.

It is worth noting that, according to the EDPB, the above assessments and activities shall be appropriately documented to have them readily available in case of request by the competent supervisory authority.

The end date for providing feedback in the context of the public consultation is December 21, 2020.

Here is the *link* to download the Recommendation.

II EDPB RECOMMENDATIONS ON THE EUROPEAN ESSENTIAL GUARANTEES FOR SURVEILLANCE MEASURES

On 10 November 2020, the EDPB also adopted the "*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*" (the "**EEG Recommendations**"), which are complementary to the Recommendations. Indeed, under Step 3 of the Recommendations, in assessing the level of protection provided by the law of the third country, a significant role is played by laws requiring personal data disclosure to public authorities for criminal law enforcement.
The EEG Recommendations are intended to provide data exporters with useful elements to assess the adequacy of the level of protection offered in the third country by the legal framework governing the access of public authorities to data for surveillance purposes.
They are reference standards, developed on the basis of European Union law, the jurisprudence of the CJEU and the European Court of Human Rights, that should be taken into account when assessing whether access to personal data by public authorities in the areas of criminal enforcement, regulatory control and national security, can be considered a justifiable interference, compliant with the fundamental rights to privacy and the protection of personal data enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

The EPDB has identified four different essential European guarantees, the existence of which makes the surveillance measures adopted by the third country justifiable, as they are deemed consistent with European standards of protection:

I. Data processing must be based on clear, precise and accessible rules. Therefore, any interference with the rights of the data subject must be justified by law, which will have to define the scope of any limitation on fundamental rights and provide for the possibility to act on these rights in case of arbitrary and abusive interference. The law must provide, *inter alia*, "*a definition of the categories of people who could be subject to surveillance, a limit on the duration of this measure, the procedures to be followed in examining, using and storing the data obtained and the precautions to be taken when communicating the data to other parties*".

II. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated. In order to be considered in conformity with the principle of proportionality, the law itself will have to identify the limitations on the power of public authorities to interfere with the rights of data subjects within the framework of surveillance programs and the limits imposed on public authorities to have access to and use the data collected, in compliance with the principle of necessity.

III. Provide for an independent and impartial oversight mechanism, provided by a judge or other independent body in relation to all phases of the monitoring activity to identify any interference with the data subjects' rights.

IV. Provision of effective remedies available to data subjects in order to ensure that they are able to exercise their rights if they believe that their rights have been violated, in order to have access to their data and to obtain their rectification or erasure. The EDPB notes that the effectiveness of such a remedy is "inextricably linked" to prior notification to the data subject of a surveillance measure once such activity has been completed. In any case, even in the absence of prior notification, an effective legal remedy must be provided. It must be a court or other impartial and independent body that takes decisions capable of binding the intelligence services.

In its final comments, the EDPB highlights how the above essential guarantees must be considered cumulatively and the evaluation of the law of the third country in light of the guarantees can lead to only two results: the legislation presents the EEG and therefore guarantees a level of protection essentially equivalent to that guaranteed in the EU or it does not.

The EEG Recommendations can be consulted *here*.

III EDPS STRATEGY FOR UNION, INSTITUTIONS, OFFICES, BODIES AND AGENCY TO COMPLY WITH THE "SCHREMS II" RULING

The EDPS is the independent supervisory authority established by Article 56 of the Regulation (EU) 2018/1725 ("**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 (2) of the Regulation.

On 29 October 2020, The EDPS issued a strategic document aiming to monitor ("Strategy") compliance of EUIs with the "Schrems II" judgement in relation to transfers of personal data to third countries, and in particular, to the United States. The goal is that ongoing and future international transfers are carried out in accordance with EU data protection law.

While the strategy in question aims to bring all transfers into compliance with the Schrems II Judgement in the medium term, the EDPS has identified two priorities to address in the short-term: ongoing controller to processor contracts and/or processor to sub-processor contracts involving transfers of data to third countries, with a particular emphasis on those carried out to the United States.

It is in this context that the EDPS has developed an action plan to streamline compliance and enforcement measures, 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 encourage s 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 – as prescribed by art. 50 of Regulation - 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. 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.

The EDPS 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.

In the end, please note that within the EDPB, the EDPS is working with the other Data Protection Authorities 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.

IV EUROPEAN COMMISSION DECISION – STANDARD CONTRACTUAL CLAUSES FOR CROSS-BORDER TRANSFERS OF PERSONAL DATA

It is no coincidence that the European Commission ("**EC**") published its draft implementing Decision[1] ("**Decision**") along with a new set of standard contractual clauses for cross-border data transfers of personal data, annexed thereto ("**Draft SCCs**"), right after the Recommendation referenced above under **paragraph I of this Newsletter**.

Below we have listed certain key points on the Decision and the Draft SCCs, whose public consultation period (expired on December 10, 2020) will be followed by the procedure for approval by EU Member States along with the opinion of the EDPB and the EDPS (s.c. "comitology")[2].

PURPOSES – The Decision addresses the following needs:

- deploy a model of standard contractual clauses aligned to the GDPR and consistent with principles enshrined in the context of *Schrems II* case (thereby superseding the existing model, anchored to the Directive 95/46/EC[3]);

[1] *Commission Implementing Decision (EU) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.*

[2] See art. 93 of the GDPR and Regulation (EU) 182/2011 (please find here the link to the description page in the EC website).

[3] Reference is made to standard contractual clauses set out in Decision 2001/497/EC, as amended, and in Decision 2010/87/EU.

- modernize the existing model *vis-à-vis* the developments in the digital economy, the widespread use of new and more complex processing operations and chains as well as the evolving business relationships;
- use a more flexible approach *vis-à-vis* the multiple scenarios and roles of data exporters and importers as well as additional parties joining the existing contractual relationships.

SCOPE – The Draft SCCs arrange general clauses with a modular approach, to cater different scenarios in which legitimacy to cross-border transfers of personal data is to be given. Most notably, they may be entered into between the following 4 pairs:

	(A)	(B)	(C)	(D)
Data exporter	Controller	Controller	Processor	Processor
Data importer	Controller	Processor	(Sub) Processor	Controller

It is worth noting that Draft SCCs:

- may be also used where the data exporter itself is not established in the EU, but the processing falls within the scope of the GDPR[4];
- allow the parties to have data processing agreements requirements (under Article 28 of the GDPR) fulfilled at once: should a data importer (processor) accept the Draft SCCs – as not negotiable and inherently not "processor-sided" – the foregoing would remove the need for a separate data processing agreement and cut down negotiations efforts;
- may be joined by additional controllers and processors – with the agreement of the original parties – acceding by completing and signing *Annexes* thereto (see further below).

CLAUSES – The body of the Draft SCCs' is divided into different modules depending on (A), (B), (C) and (D) pairs depicted in the above chart. However, core obligations and principles remain unaffected across the modules (*e.g.* provisions related to transparency, security, storage limitation, minimization, enforceable rights and effective legal remedies for data subjects etc.) as mirroring GDPR ones which, therefore, become contractually binding upon data importers outside of its scope. In this regard:

- the parties remain free to include the Draft SCCs in a wider contract as well as to add other clauses or safeguards, the latter supplementing and compatible with those outlined by the Draft SCCs (the EC even encourages the parties to provide additional safeguards);
- beyond relying on Draft SCCs, the data exporter has to fulfil its general responsibilities as controller or processor in accordance with the GDPR (*e.g.* to provide data subjects with adequate information);
- the parties should be able to demonstrate compliance with the Draft SCCs, most notably: (i) the data importer shall keep appropriate documentation for the processing activities under its responsibility and promptly inform the data exporter if it is unable to comply with the Draft SCCs; (ii) the data exporter shall suspend the transfer and, in particularly serious cases, have the right to terminate the related contract where the data importer is in breach of, or unable to comply with, the Draft SCCs.

ANNEXES – The Draft SCCs contain the following *Annexes* to be duly filled in and executed by the parties:

- *Annex I.A – List of Parties* – to include identification data of relevant parties to the Draft SCCs.

[4] Namely, where the processing is related to *(a)* offering of goods or services to data subjects in the EU or *(b)* monitoring of behavior of data subjects in the EU as far as it takes place within the EU (art. 3, par. 2 of the GDPR).

- *Annex I.B – Description of the transfer(s)* – to provide details of the processing activities related to the transfers (*e.g.* categories of personal data involved, purposes for which they are transferred, storage period etc.).
- *Annex II – Technical and organizational measures* – to outline technical and organizational security measures to be implemented by the data importer. Security requirements are pivotal to the Draft SCCs, as also appearing by the articulated list of exemplary security measures provided by the EC (by which it has implicitly pointed out its expectations).
- *Annex III – List of Sub-Processors* – to indicate the sub-processors – either already authorized by the data exporter (where it granted the importer with a specific prior authorization) or intended to be engaged by the data importer (where it was granted by the exporter with a general authorization) – in any case to be kept up to date.

FOREIGN LAW – It should be noted that entering into Draft SCCs would not relieve the exporter from undertaking its assessment concerning the laws applicable to the data importer – as also outlined under the Recommendation (**see above under paragraph I of this Newsletter**) – the Draft SCCs rather designing a general framework of duties and mandatory steps to carry out such assessment and to manage critical situations (*e.g.* requests from foreign law enforcement or intelligence agencies).

At the time of agreeing upon Draft SCCs, the parties should make certain that they have no reason to believe that the laws applicable to the data importer are not in line with requirements under the Draft SCCs.

TRANSITIONAL PERIOD – During a transitional period of 1 year – from the date of entry into force of the Decision – exporters and importers may continue to rely on the existing model of standard contractual clauses, so long as:

- it is for the performance of a contract concluded between them before the abovementioned date;
- during the transitional period, the contract remains unchanged, except for necessary supplementary measures (see above under paragraph I of this Newsletter).

The necessity of adopting the new Draft SCCs during the transitional period, where triggered at the controller/processor level, will have a trickle-down effect at the processor/sub-processor one.

Following the transitional period or outside the "exempting" circumstances highlighted above, the actors concerned should take on a re-papering of existing contracts and enter into the new Draft SCCs in order to comply with data protection laws.

V FIRST "POST-SCHREMS II" DECISION RELATING TO PERSONAL DATA TRANSFERS ISSUED BY THE SWEDISH DATA PROTECTION AUTHORITY

On December 11, 2020 the Swedish DPA issued an administrative fine against the Umeå University for violating various GDPR provisions due to these shortcomings:

I. lack of adequate security measures for the protection of special categories of personal data and other sensitive information (also concerning sexual life and health of data subjects) contained in over a hundred preliminary investigation reports on male rape cases. Such reports – previously requested from the police by a research group at the University – were digitally scanned and stored in a **US-based cloud** (despite contrary indication of the University, as published on its intranet portal);

II. repeated dispatch of unencrypted e-mails with the scanned reports attached thereto (despite explicit contrary indication of the police);

III. failure to notify to the Swedish DPA about certain personal data breaches occurred as well as failure to point out the measures implemented in order to mitigate the effects thereof, on the one hand, and to prevent similar incidents from happening in the future, on the other hand.

The decision is noteworthy as the first concerning cross-border transfers of personal data after Schrems II ruling and explicitly mentioning it (albeit "not applicable" at the time of the events at stake, when the EU-US Privacy Shield was still in force).

In particular:

- the Umeå University stored the data by using a cloud service provided by a company established in the United States, which at that time (spring 2019) had declared to be in compliance with the EU-US Privacy Shield. Although the transfer as such has to be considered permitted on the basis of the EU-US Privacy Shield, the Swedish DPA remarked how the processing and storing of such sensitive data should not be carried out by using a cloud service with such features and that the measures adopted by the Umeå University – *inter alia* the implementation of a single-factor authentication process to access the network – could not be considered adequate to prevent third party from accessing the data.
- the Swedish DPA points out how the data transfers to third countries outside the EEA increase the risk for personal data since – *inter alia* – the data subjects may be prevented from enforcing their rights or from prohibiting unauthorized disclosure or access to personal data transferred, thereby requiring additional burden on the controllers and processors as to the measures required to comply to the GDPR.

Given the current "state of the art" after the Schrems II ruling, it is crucial for controllers and processors to prove the adoption of adequate measures to make data transfers compliant to GDPR taking into consideration the whole set of guidelines and provisions recently adopted by the various EU Authorities (as summarized in the above paragraphs).

Contacts

Gilberto Nava
Partner – Chiomenti
IP, TMT, Data Protection
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Giulio Vecchi
Counsel – Chiomenti
IP, TMT, Data Protection
T. +39.02.72157.658
giulio.vecchi@chiomenti.net