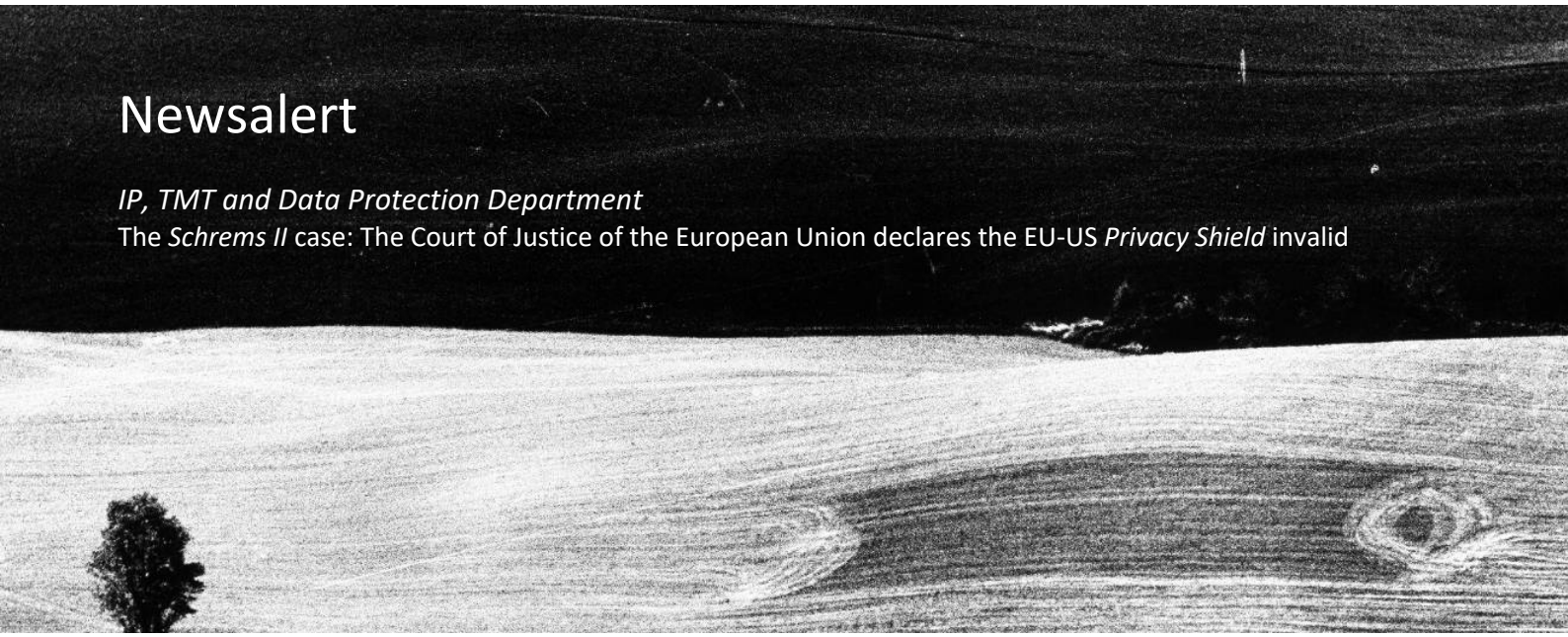
CHIOMENTI



Newsalert

IP, TMT and Data Protection Department

The *Schrems II* case: The Court of Justice of the European Union declares the EU-US *Privacy Shield* invalid

PRIVACY SHIELD EU-US: IN THE BACKGROUND OF THE *SCHREMS II* CASE

On 16 July 2020, the Court of Justice of the European Union ("**ECJ**") ruled again on transfers of personal data to the U.S.A. in the *Schrems II* case (Case C-311/18). The ruling stemmed from a referral of the Irish High Court, following a complaint brought by Maximilian Schrems, an Austrian citizen who had requested the Data Protection Commission (i.e. the Irish supervisory authority) to prohibit the transfer by Facebook Ireland Limited of his personal data to the U.S.A., on the grounds that U.S.A. law and practice did not provide sufficient protection.

In particular, the recent ruling of the ECJ concerned the Decision (EU) 2016/1250 of the European Commission which, as is well known, had established the so-called EU-US Privacy Shield ("**Privacy Shield**"), attesting that the U.S.A. would ensure an adequate level of protection of personal data transferred from the countries of the European Economic Area ("**EEA**") to companies and organizations certified under this program.

In the case at hand, however, the ECJ ruled that Decision (EU) 2016/1250 is invalid since the Privacy Shield does not guarantee *de facto* compliance by the U.S.A. with the principle of adequacy of the level of protection of personal data transferred from the EEA, as set out in Regulation (EU) 2016/679 ("**GDPR**").

Notably, the ECJ affirmed that the Privacy Shield, also in the light of the fundamental principles enshrined in Artt. 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, does not represent an adequate solution under two distinct aspects. On the one hand, since it provides for the prevalence, in the U.S.A. legal system, of the requirements relating to national security and public interest over the fundamental rights of the citizens – a circumstance which is able to determine interferences in the context of public controls and intelligence's activities and result in a violation of the principles of necessity and proportionality imposed by the laws of the EU. On the other hand, the ECJ highlights that the U.S.A.A legislation on which surveillance and intelligence programs are based does not grant to the EU citizens concerned any rights against U.S.A. authorities that can be enforced before judicial bodies, thus frustrating their right to an effective judicial remedy.

The assumptions on which the ECJ had already declared the invalidity of European Commission Decision 2000/520 on the so-called Safe Harbor framework in the *Schrems I* case (Case C-362/14) were therefore confirmed *mutatis mutandis*.

WHAT ARE THE ALTERNATIVES TO THE PRIVACY SHIELD TO TRANSFER PERSONAL DATA TO THE U.S.A.?

The judgment of the ECJ urges the need, for economic operators and international organizations intending to transfer personal data towards the U.S.A., to resort to alternative instruments providing appropriate safeguards (Art. 46 of the GDPR) or to specific derogations (Art. 49 of the GDPR), similarly to what is provided for other third countries which are not recipients of an adequacy decision of the European Commission. It should be noted, in fact, that the circumstances that the ECJ did not grant any "grace period" resulted *ipso facto* in any transfer to the U.S.A. based on the Privacy Shield mechanism being illegitimate, as also restated by the European Data Protection Board ("**EDPB**") in its preliminary guidance[1] issued in relation to the *Schrems II* ruling. Please find listed below the possible alternative solutions in the light thereof.

[1] Please refer to the "*Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*" adopted by the EDPB on 23 July 2020 ("**FAQ**").

(A) STANDARD CONTRACTUAL CLAUSES

In the *Schrems II* judgment, the ECJ also ruled on one of the best-known instruments providing for appropriate safeguards, namely the so-called Standard Contractual Clauses ("**SCC**") established by Decision (EU) 2010/87, reaffirming their validity but stressing the circumstance of their limited effectiveness in relation to *inter partes* relationships, i.e. between the data exporter and the data importer.

In this view the ECJ acknowledged that, while it is true, on the one hand, that SCC have the effect of contractually binding the data importer to a level of protection of personal data in line with the requirements of EU law – imposing an obligation for the parties to verify in advance compliance with such a level in the law of the third country, with the correspondent obligation of the data importer to inform the data exporter of any impeding circumstances, and of the data exporter to suspend the transfer and/or terminate the contractual relationship – on the other hand, they do not create a legal constraint on the third country of reference.

Following the ECJ judgement, therefore, SCC still appear in principle to be a valid instrument with a view to lawfully transfer personal data to third countries. However, in concrete terms, this instrument entail the risk not to be sufficient in itself, in the absence of public law and not merely contractual safeguards, to lawfully transfer personal data to the U.S.A. or other third countries where mass surveillance policies or other circumstances do not ensure, *de facto*, a principle of essential equivalence with the rights' protection guaranteed under EU law.

In this regard, the EDPB itself – also extending the reference to all SCC models issued by the European Commission[2] – restated the obligations to assess the circumstances surrounding the transfer (i.e. to determine whether the SCC constitute, in each given case, an instrument offering adequate safeguards), if necessary by taking appropriate measures in addition to SCC. Where, despite the supplementary measures adopted, the law of the third country should nevertheless interfere to such an extent as to affect the conceived guarantees, the data exporter will have to opt for a suspension or termination of the transfer or, if it intends to continue the transfer, notify the competent supervisory authority[3].

(B) BINDING CORPORATE RULES

Appropriate safeguards also include Binding Corporate Rules, which are used to allow transfers of personal data between members of the same group of undertakings or of enterprises engaged in a joint economic activity (e.g. multinational groups with complex data flows). Binding Corporate Rules must comply with the requirements of Art. 47 of the GDPR and be approved in advance by the competent supervisory authority or the lead supervisory authority, following the opinion of the EDPB.

Although the *Schrems II* judgement did not rule directly on this instrument, also the Binding Corporate Rules would be affected by the ECJ's judgement as stated by the EDPB[4], which extended to the Binding Corporate Rules the same conclusions concerning the obligations imposed on the parties that the ECJ drawn with reference to the SCC.

(C) CODES OF CONDUCT, CERTIFICATION MECHANISMS AND OTHER INSTRUMENTS

Eventually, also codes of conduct and certification mechanisms constitute appropriate safeguards for the transfer of personal data to third countries - these are peculiar instruments of potential interest for those who process personal data, which, however, remain at present a mere regulatory provision pending effective implementation – as well as the other instruments set forth under Art. 46 of GDPR[5]. While deferring any *ad hoc* remarks at a later stage, the EDPB restated also for the above instruments the need that the principle of the adequacy of the level of protection of personal data is not affected by extra-EEA transfers.

(D) DEROGATIONS

As regards the cases of derogation, Art. 49 of the GDPR provides that – in certain circumstances set forth exhaustively – a transfer of data to third countries may be regarded as lawful even in the absence of an adequacy decision and of appropriate safeguards. That may be the case, in particular, where: *(a*) the data subject has **explicitly consented** to the proposed transfer; *(b)* the transfer is necessary for the **performance of a contract between the data subject and the controller** (or the implementation of pre-contractual measures taken at the data subject's request); *(c)* the transfer is necessary for the **conclusion or performance of a contract concluded in the interest of the data subject** between the controller and another natural or legal person; *(d)* in further cases where the transfer is necessary, by way of example, for the exercise legal claims, for important reasons of public interest, for the protection of the vital interests of the data subject.

---

[2] See FAQ n° 5). Most notably, reference is to the other models of SCC referred to in Decision (EC) 2001/497 (see *ANNEX - Clause 5, let. a)*) and Decision (EC) 2004/915 (see *ANNEX - Point II. c)),* relating to transfers of personal data where both the data exporter and the data importer act as data controllers, whereas the SCC referred to in Decision (EU) 2010/87 (see *ANNEX - Clause 4(g)*) – concerned by the ECJ judgment at hand – relate to transfers where the data exporter and the data importer act as data controllers and data controller, respectively.

[3] See above.

[4] See FAQ n° 6).

[5] See. FAQ n° 7). Reference is made, among others, to further SCC models that may be approved by national supervisory authorities and the European Commission, as well as to provisions to be inserted into administrative arrangements between public authorities or bodies authorized by the competent supervisory authority (in this case with the application of the consistency mechanism provided for in Article 63 of the GDPR).

Finally, where none of the above exceptions apply, processing operations necessary for the purposes of pursuing a compelling legitimate interests of the data controller, where they override the interests or rights and freedoms of data subjects, are not repetitive and relate to a limited number of data subjects, shall be permitted.

It should be noted, however, that the latter scenario, as well as all the derogations provided for in Art. 49 of the GDPR, are subject to individual limitations and must comply with specific parameters. In particular, the EDPB clarified *inter alia* that these exceptions must be understood in a restrictive and residual way with respect to the possibility of using one of the instruments referred to in Art. 46 of the GDPR, and that some of them (for example, those relating to the performance of a contract or the exercise of a right) apply in any case only to "occasional" transfers[6].

The assessment of the existence and applicability of these derogations will therefore have to be made on a case-by-case basis in the light of the concrete circumstances of the transfer.

* * *

The issuing of further guidance following the *Schrems II* ruling is currently under examination by the EDPB, who exhorted the supervisory authorities to follow a coordinated approach[7], in particular as regards the obligations on data exporters and importers to assess the adequacy of the protection afforded by the third country and to provide for measures additional to those included in the SCC, including the concrete definition of what those measures might consist in.

Pending such indications – and hopefully an updated version of the SCC , given the obsolescence of the current versions emerging, for example, by the references to the repealed Directive 95/46/EC – in the light of the caveats already set out by the EDPB[8], it seems appropriate that the organizations concerned take certain actions with regard to their transfer activities, both to the U.S.A. and to other non-EEA countries not covered by an adequacy decision of the European Commission.

Such actions should include: ***(i)*** a review of the transfers performed, either directly or through data processors (possibly by negotiating appropriate amendments to the agreements in place with the latter), taking into account the different situation that may constitute a "transfer", especially by electronic means (*e.g.*, remote access by an entity located in a third country, for administration or maintenance purposes[9]); ***(ii)*** a case-by-case determination of the obligations of exporters and importers, both with regard to the prior assessment of the adequate level of protection by the third country and the need to implement any supplementary measures aimed at remedying the absence of an adequate level of protection (*e.g.*: periodic reporting and information obligations of the *data importer*, advanced encryption measures and so-called “tokenization” of personal data); ***(iii)*** depending on the circumstances relating to the third country concerned, where the adoption of such measures would not be sufficient to mitigate factors affecting the safeguards provided, opting for a suspension or termination of the transfer or, otherwise, notifying the competent supervisory authority of the intention to keep the transfer in place.

Granted all the above, it seems fair to wonder, however, whether and to which extent – even in the light of the accountability principle underlying the GDPR - economic operators are indeed best placed to carry out assessments of the adequacy of the level of protection provided by the third countries, and whether this does not result in an unproportionate burden in terms of resources for the operators themselves.

The overall framework outlined so far following the *Schrems II* judgement raises further questions about the actual organizational capability of the supervisory authorities to deal with all notifications from economic operators intending to continue with transfers of personal data which, while at risk in terms of level of protection afforded, may be essential for their business activities.

Contacts

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

Giulio Vecchi
Counsel – Chiomenti
IP, TMT and Data Protection Department
T. +39.0272157658
giulio.vecchi@chiomenti.net

[6] See FAQ n° 8). The matter has been thoroughly examined by the EDPB in its "*Guidelines 2/2018 on exceptions under Article 49 of Regulation 2016/679*".

[7] See FAQ n° 9).

[8] See in particular FAQ n° 9) to 12), granted what stated above.

[9] See FAQ n° 11).