ECIJA

July 2020

Privacy Shield's invalidation: guide on how to act when transferring international data to the US

Report

Privacy and Data Protection Area

www.ecija.com

ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Court of Justice of the European Union invalidates "Privacy Shield" and expresses reservations towards Standard Contract Clauses

We recently became aware of the Judgement of the Court of Justice of the European Union (hereinafter "CJEU") dated July 16, 2020, in Case C-311/18 Facebook Ireland v. Schrems, which invalidated the Commission Implementing Decision (EU) 2016/1250 of July 12, 2016, on the adequacy of the protection provided by the EU-US Privacy Shield (hereinafter "***Privacy Shield***").

(I) ANALYSING THE IMPACT OF THE JUDGEMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION WHICH INVALIDATES THE PRIVACY SHIELD

This Judgement **directly affects all companies, administrations and institutions that, directly or indirectly, communicate personal data or make them available to US entities adhering to the Privacy Shield, whether for the purpose of a service provision, a data transfer, or because their parent company or other group companies to which information containing personal data must be reported are based in the US and the lawfulness of that transfer stands on the Privacy Shield.**

The CJEU does not establish a grace period for companies to embrace this new situation and reaches a series of conclusions regarding international data transfers:

(i) Invalidation of the Privacy Shield

1. **The CJEU considers that it is invalid** as an adequacy decision, taking into account that it does not guarantee the minimum level of protection required by Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter '***GDPR***'), since the **data subjects whose personal data are transferred outside the EU are not granted effective and enforceable rights and the channels established for administrative remedies and judicial proceedings are not effective**.

2. It should be recalled that adequacy decisions are based on the equivalence, in terms of respect for data protection, of the legal framework prevailing in the State of the importer with that applicable in the State of the exporter, i.e. that it respects the content of the Charter of Fundamental Rights of the European Union.

   In this sense, the CJEU understands that the **wording of the Privacy Shield limits the application of the essential principles for the processing of personal data concerning European citizens as it allows US authorities to require disclosure of such data where certain circumstances are given, that taking precedence over the principles established in the data protection regulations applicable in the European Union**.

3. This limitation constitutes an **interference with the rights and freedoms recognized by the Charter of Fundamental Rights** referred to above. Thus, the CJEU establishes that the interferences derived from surveillance programs based on section 702 of the *Foreign Intelligence Surveillance Act* and *Executive Order 12333* are not covered by the requirements that ensure, subject to the principle of proportionality, a level of protection equivalent to that guaranteed by the European Charter, as well as the surveillance programs based on the terms of *Presidential Policy Directive 28, in* respect of which the US Government itself has accepted that the rights of the data subjects cannot be exercised before the Courts against the US Authorities.

4. The CJEU concludes that a legislation which does not provide for any possibility for a natural person to seek judicial remedies to access his/her personal data or to obtain the rectification or erasure thereof does not respect the fundamental right to the effective judicial protection and is incompatible with the level of protection required by the European Union's legal framework.

5. In addition, it establishes that the figure of the Ombudsman is not sufficient to guarantee the legal protection of the data subjects since

    - It is not independent as it must report to the U.S. Secretary of State.
    - It has no mechanisms to ensure compliance by the intelligence services.

(ii) On the validity of the Standard Contractual Clauses

1. The CJEU also ruled on the standard contractual clauses for the transfer of personal data to processors located in third countries (hereinafter "***SCC's***") amended by the Commission Implementing Decision (EU) 2016/2297 of 16 December 2016, stating that, **although they are valid, additional safeguards will sometimes be necessary**.

    In this way, the CJEU understands that the use of the SCC's entails the need to guarantee a level of protection equivalent to that required by the GDPR and the European Charter of Human Rights. However, **not only should the content of the SCC's be taken into account, but also whether the legal framework in the destination country allows for compliance**. In this sense, among the other aspects, an assessment should be made as to whether the destination country provides regulations or guarantees in relation to the protection of privacy and personal data, and their degree of development and implementation.

2. The CJEU understands that these contractual clauses **do not bind the Authorities of the country of destination, since they do not form part of the agreement**. Therefore, even if they are correctly signed, they should not be automatically considered to be providing adequate guarantees as there is no certainty that the Authorities of the State of the recipient cannot access the information, nor that the data subjects have effective legislative mechanisms for the defense and exercise of their rights.

3. As a control measure, the CJEU states that **a Supervisory Authority must prohibit/suspend an international transfer of data based on SCCs where a level protection equivalent to that of the GDPR is not guaranteed in the country of destination**.

This power of prohibition/suspension should not be understood as exclusive of the Supervisory Authorities, since the exporters of the information themselves, supported by the recipients, are recognized as having the possibility of cancelling international transfers when they observe that, for whatever reasons, it is not possible to guarantee a level of protection of personal data equivalent to that required by the RGPD.

This framework **would exempt those countries or regions that already have an adequacy decision from the European Commission** (Switzerland, Canada, Argentina, Uruguay, Guernsey, Isle of Man, Jersey, Faeroe Islands, Andorra, Israel, Uruguay, New Zealand and Japan).

4. The CJEU establishes that those **businesses processing personal data must address the definition and establishment of additional measures for the safeguard of adequate guarantees and**, only in a subsidiary case, must such measures be entrusted to the corresponding Supervisory Authority. This ruling does not determine the nature of these additional measures conceived to provide guarantees that cannot be undermined even by the authority of the State receiving the information.

5. The obligation established by the SCC's to **report the data controller any impediment to complying with the** SCC's was also recalled. **This obligation should also apply with respect to any regulatory change that recipient of the information considers may prevent it from complying with the obligations established in the SCC's**. In such cases, the data already transferred to the third country in question must be returned and all copies of such data must be returned or destroyed.

   In this case, **if the data controller does not cease the international transfer, it must notify the competent supervisory authority so that it can audit the recipient and decide, in the light of its particular context, if the transfer should be prohibited** on the grounds that an adequate level of protection is not guaranteed.

6. By way of clarification, it should be noted that the CJEU makes these considerations with regard to the (i) Decision on the adequacy of the Privacy Shield which affects any kind of relationship (Controller to Controller, Controller to Processor, etc.) and (ii) Commission Decision of February 5, 2010, which **only regulates the relationship of the Controller with a Processor.** That being said, the analysis carried out by the CJEU is focused on the lack of security of the regulations of the country importing the personal data, so the above-mentioned considerations, as well as the ones analyzed below, **should apply regardless of the relationship** between the parties.

(II) PRONOUNCEMENTS BY THE SUPERVISORY AUTHORITIES

As a result of the Resolution of the CJEU, different Data Protection Authorities have expressed their opinion on how this new scenario should be approached by European companies, administrations and institutions, taking into account both its impact in relation to the protection of the data concerning European citizens and from the perspective of the economic relations between Europe and the United States, valued at 7.1 billion dollars and directly affecting the 5,300 US companies adhered to the system invalidated by the CJEU.

(i) European Data Protection Bureau

The European Bureau has expressed very briefly the need to analyze what the additional measures referred to in this note might consist of:

1. Assessment (with the assistance of the importer if necessary) of whether the countries to which the data are sent offer adequate protection. Taking into account:

    a. The contents of the SCC's.
    b. The specific circumstances of the transfer; and
    c. The legal regime applicable in the importer's country, the analysis of which shall be carried out in the light of the non-exhaustive factors set out in Article 45.2 of the GDPR.

2. Establishment of measures additional to those included in the SCC's if the result of this assessment is that the country of the importer does not provide a level of protection equivalent to that established in the EU. These measures have not been reported or specified yet by this body.

(ii) European Data Protection Supervisor

The EDPS has expressed similar views in its *DPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems.* In this respect, the EDPS welcomes the decision reached by the CJEU regarding the invalidity of Privacy Shield and highlighting the need to recognize the possibility to claim and/or exercise rights.

While recognizing the validity of the SCC's as a measure to provide adequate safeguards for the performance of an international transfer, in the absence of an Adequacy Decision, it has not yet provided additional information on the possible additional measures set out by the CJEU.

(iii) Germany

The Federal Commissioner, in his statement on the Resolution, has stressed that international data transfers are still possible and that special protection measures must be adopted for transfers with the United States.

For its part, the Berlin Authority requested in its declaration that the controllers who carried out international data transfers to the United States should transfer them to Europe, maintaining a standard of legal security until the US-EU legal framework is reformed. In

relation to the use of SCC's, it stressed the obligation to check before the first data transfer whether the third country has State access to the data which goes beyond what is allowed by European legislation and whether such access rights exist, among other aspects.

In this regard, the Berlin Commissioner for Data Protection and Freedom of Information has indicated that data controllers who transfer personal data to the United States are now obliged to immediately switch to service providers in the European Union or in a country with an adequate level of data protection.

(iv) The Netherlands

The Dutch Supervisory Authority has stated that EU organizations should not, for the time being, simply transfer personal data to the United States, pointing out that the Commission should establish a new regime for such transfers.

(v) Ireland

The Irish Authority has expressed the need to adopt mechanisms to ensure that international transfers are made to countries with a level equivalent to that of the European Union, questioning the practical validity of the SCC's as long as these requirements cannot be effectively guaranteed.

(vi) Liechtenstein.

The Data Protection Authority in its statement on the Judgement informed that it would analyze the consequences for data transfers to third countries and, in addition, issue further instructions. Furthermore, it stressed that, until a new instrument is agreed with the US, companies will have to rely on the safeguards set out in Article 46 of the GDPR, including the SCC's.

(vii) Other European Union member States.

The rest of the Supervisory Authorities of the European Union member States, as is the case of Spain, have expressed themselves in the sense that they are analyzing the Judgement, as well as the need to address new mechanisms and to review their impact on other mechanisms such as the SCC's.

(viii) The position of the United States.

Because of its relevance to this issue, the **US Secretary of Commerce**, which claims to maintain close contact with the European Commission and with the European Data Protection Bureau, should be taken into account, as well as its intention to continue to administer the Privacy Shield program, including the processing of self-certification and re-certification applications, with the understanding that the CJEU's Judgement does not exempt the listed organizations from previously acquired obligations.

(III) CONCLUSIONS AND THE WAY FORWARD FOR THE REGULARIZATION OF INTERNATIONAL DATA TRANSFERS TO THE UNITED STATES

In view of the current situation and in order to analyze the impact of the Judgement on companies, administrations and institutions performing international data transfers to the United States, the following conclusions can be drawn:

1. The first aspect to remember is the **loss of the Privacy Shield, which prevents international transfers to entities established in the United States based on this mechanism**.

2. According to the provisions of the GDPR, in the absence of an Adequacy Decision other or adequate safeguards, the transfer or set of transfers of personal data to a third country or international organization shall only take place if one of the following conditions are met:

    - **The data subject has explicitly given his/her consent to the proposed transfer, after having been informed of the possible risks of such transfers due to the absence of adequate safeguards**.
    - The transfer is **necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject** (e.g. a service directly contracted with an entity outside the European Economic Area).
    - The transfer is **necessary for the conclusion or performance of a contract, in the interest of the data subject,** between the controller and another natural or legal person (with the same proviso as above).
    - The transfer is **necessary for important reasons of public** interest (which must be duly justified).
    - The transfer **is necessary for the formulation, exercise or defense of claims**.
    - The transfer is **necessary to protect the vital interests of the data subject or of other persons,** where the data subject is physically or legally incapable of giving consent.
    - The transfer **is made from a public register which, in accordance with Union law or the law of the EU member States, is intended to provide information to the public and is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest,** but only insofar as the conditions laid down in Union law or the law of the EU member State are fulfilled in the particular case.

3. Before international data transfers are carried out, it must be **assessed whether the countries to which the data are sent offer adequate protection**. If this is not the case and the data transfer is based on the signing of the SCC's, additional

measures to the SCC's should be provided to ensure such compliance. In this sense, recital 109 of the GDPR includes the possibility of modifying the SCC's provided that it is to extend the guarantees and obligations therein.

4. In the absence of an Adequacy Decision, the appropriate guarantees provided for in the regulations in force and specifically in Articles 44 to 49 of the GDPR must be granted:

    - **SCC's currently in force may be used incorporating additional guarantees.**
    - **Establishment and approval of Binding Corporate Rules.**
    - **Codes of conduct together with binding and enforceable commitments** from the controller or processor in the third country to implement appropriate safeguards, including those relating to the rights of data subjects.
    - **Approved certification mechanism** together with binding and enforceable commitments by the controller or processor in the third country to apply appropriate safeguards, including those relating to the rights of the data subjects.
    - **Request the corresponding administrative authorization to a competent Supervisory Authority**.

5. Companies must **implement mechanisms to obtain information regarding the suitability of the data importer or the possible transfers,** issues that were already included in the GDPR in relation to the guarantees to be analyzed when selecting a supplier.

6. **The definition and implementation of such additional guarantees are the responsibility of both the exporter and importer of the data**. Although the corresponding Supervisory Authority may have an ancillary duty to foster such actions.

    They should, for example, establish mechanisms for assessing the adequacy and level of compliance or the need to update them at the discretion of the European Authorities and possible new European Decisions.

    Recital 109 of GDPR already provides for the possibility for the controller or processor to strengthen the measures set forth in the SCC's by including them in a wider contract, **adding additional clauses or guarantees, provided that they do not directly or indirectly contradict the SCC's adopted by the Commission or by a Supervisory Authority, nor undermine the fundamental rights or freedoms of the data subjects**.

    In any case, the adoption of these additional guarantees should aim at avoiding that the reasons that have led to the invalidation of the Privacy Shield may concur again, ensuring that undue access to personal data by the third country is avoided and that effective defense mechanisms for both the exporter and the data subjects are guaranteed.

7. The failure to adopt sufficient guarantees **may lead, together with possible sanctions arising from carrying out international transfers of data without sufficient guarantees, to the immobilization or blocking of the data, the right of the data subject to receive compensation for the damage suffered and to reputational damages to the companies involved.**

8. In the event that international data transfers are not regularized, we must remember that, in accordance with Article 72 of Spanish Organic Law 3/2018, of

December 5, on the Protection of Personal Data and the Guarantee of Digital Rights, **the international transfer of personal data to a recipient in a third country or to an international organization, when the guarantees, requirements or exceptions established in the GDPR are not met, may lead to economic sanctions of up to 4% of the global turnover or up to 20 million Euros.**

Area of Privacy and Data Protection
+ 34 91 781 61 60
info@ecija.com


ECIJA
EXPANSIÓN
2016, 2017,
2018 & 2019
Most innovative Project
Best Economy
Digital Firm
FT
FINANCIAL TIMES
FINANCIAL
TIMES
2019
Among the 20
most innovative
European Firms
TOP RANKED
Chambers
EUROPE
2019
The LEGAL 500
-2019-
Band 1 in TMT by
Chambers & Partners
and Legal 500
THE LAWYER
2019
Best TMT
European Firm
Forbes
FORBES
2017
Best Technological
Spanish Firm
Torre de Cristal
Pº de la Castellana, 259C
28046 Madrid