

JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION DECLARING DECISION 2000/520 OF THE COMMISSION ON THE SAFE HARBOR PRINCIPLES INVALID

The [judgment](#) of the Court of Justice of the European Union ("CJEU") declaring [Decision 2000/520 of the Commission of 26 July](#) ("**Decision 2000/520**") invalid was published on 6 October 2015. According to Decision 2000/520, US entities which had adhered to the "Safe Harbor" principles were considered to be offering adequate guarantees for international personal data transfers from European Union Member States to such US entities.

ORIGIN OF THIS JUDGMENT

The judgment solves a preliminary ruling submitted by the Irish High Court within the context of a proceeding initiated by Mr. Maximilliam Schrems against the Irish data protection authority (the Data Commissioner Officer). Mr. Schrems challenged a decision of the Irish authority that refused to investigate a complaint made by him regarding whether the transfer of his personal data by Facebook Ireland Ltd. to the US and the storage of this data on servers located there was in accordance with the EU data protection rules.

THE DECISION

The CJEU has ruled the following:

- **That Decision 2000/520 is invalid.** The CJEU based its decision, among other reasons, on the grounds that Decision 2000/520 does not provide effective legal protection against potential interference and massive processing of data by the US public authorities, which may violate the fundamental rights of European citizens whose data have been transferred to the US. The CJEU has declared this decision invalid without establishing any time limits to its effects.
- **That the existence of a Decision** in which the European Commission considers that a third country provides an adequate level of protection **does not prevent the data protection supervisory authorities of Member States** (in Spain, the Spanish Data Protection Authority ("SDPA")) **from examining and investigating a claim filed by a data subject** challenging the level of protection that has been given to his or her personal data which have been transferred to a third country, when the data subject contends that the law and practices in force in that third country do not ensure an "adequate" level of protection.

SIGNIFICANCE OF THIS JUDGMENT

As a result of this judgment the Irish High Court will require the Irish supervisory authority (Data Commissioner Officer) to examine Mr. Schrems' complaint with all due diligence and, once it has investigated all the facts, decide whether, pursuant to the directive, the transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data.

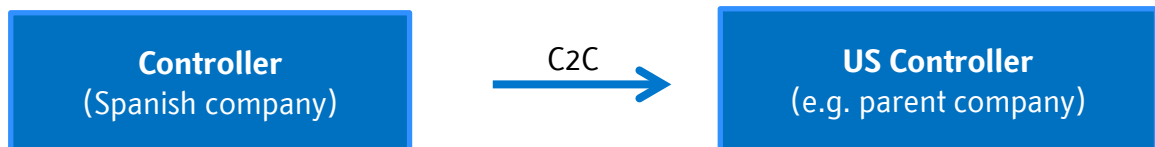
HOW THIS DECISION AFFECTS SPANISH COMPANIES THAT HAVE TRANSFERRED DATA ABROAD ON THE BASIS OF DECISION 2000/520

Decision 2000/520 being declared invalid significantly affects most of the European business sector, including Spain, giving rise to a situation of uncertainty for Spanish entities which, to date, are transferring data abroad to entities which have adhered to the Safe Harbor principles on the assumption that these entities provide an “adequate” level of protection. Once Decision 2000/520 is declared invalid, these US entities are no longer considered to be providing an “adequate” level of protection and thus Spanish companies must seek alternative legitimate ways of carrying out such transfers.

WHAT THEN SHOULD WE DO IF WE HAVE BASED OUR TRANSFERS ON SAFE HARBOR PRINCIPLES?

Although the SDPA and the European data protection authorities have not yet given any guidelines on how to facilitate compliance with data protection laws by European businesses affected by this judgment, the alternatives offered by the Spanish data protection legislation are the following:

(i) International transfers between controllers (*controller-to-controller* or **C2C**):



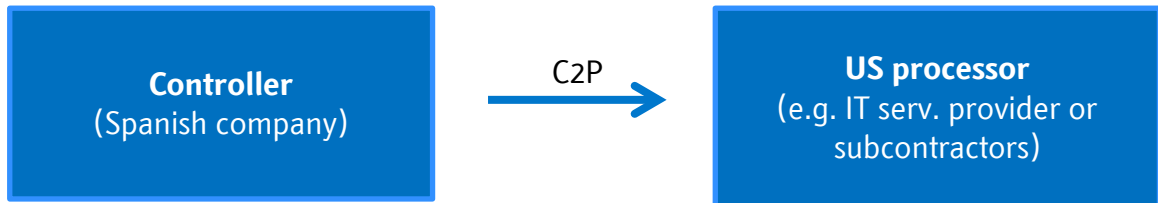
This type of transfers between controllers are made, for example, between a company subject to Spanish data protection law and its US parent company, when the parent company is to independently make decisions about the data transferred (e.g. centralised human resources decisions regarding employees of the Spanish subsidiary). In these cases, as an alternative to the Safe Harbor scheme, such transfers could be made on the following grounds (i) the transfer is necessary to execute an existing contractual relationship with or in the interest of the data subject –article 34(f) and (g) of the Spanish Data Protection Law– or; (ii) by obtaining the data subject’s unambiguous consent – article 34(e) of the Spanish Data Protection Law –.

This second alternative (consent) may not be suitable in practice taking into account:

- the free and revocable nature of the consent (is it technically and organisationally possible not to transfer the relevant data of those data subjects who have not consented to the transfer? will the company be able to manage potential revocations of consent during the term of the transfer?), or
- the number of data subjects involved in the transfer, which could in practice entail the mass management of the collection of unambiguous consents from all data subjects.

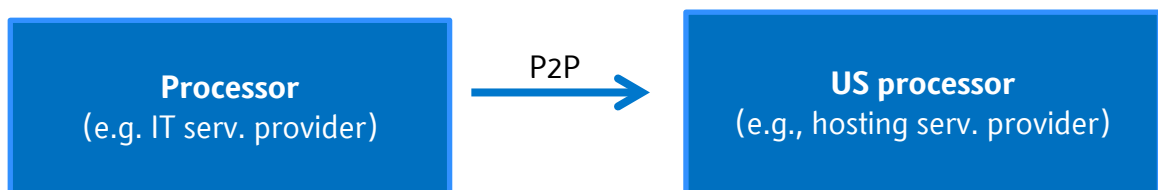
This type of transfer can also be based on other legitimate grounds, such as obtaining the prior consent from the Director of the SDPA or implementing intragroup Binding Corporate Rules or BCRs. However, in the case of BCRs, the implementation procedure is lengthy and complex and may not be the best option in the short or medium term.

(ii) International transfers between controllers and processors (*controller-to-controller* or C2P):



These transfers are carried out between a business subject to Spanish data protection law and a service provider established in the US that can access personal data (regardless of whether or not it belongs to the group). These transfers exist not only when EU companies hire US providers but also regarding their respective subcontractors located abroad. In these cases, it seems that the SDPA's authorisation is the most practical legal ground to carry out these transfers legitimately in the short term over other options such as BCRs. Also, the selection and provision of services by a supplier cannot depend on the data subject's unambiguous consent and it would also be difficult to ground the transfer on the basis that it is needed to execute an agreement with the data subject.

(iii) International transfers between processors (*processor-to-processor* or P2P):



These transfers are carried out between service providers subject to Spanish law who decide to outsource part of their services to third parties located in the US (e.g. IT service providers that subcontract hosting services to third parties). In Spain, but not in all Member States, these transfers among processors can be carried out with the SDPA's prior authorisation. Therefore, this is an option for Spanish companies contracting services from suppliers which have obtained this authorisation to transfer data to US subcontractors.

HOW ARE THE NATIONAL AUTHORITIES AND EUROPEAN INSTITUTIONS EXPECTED TO REACT?

At the time of this newsletter there has been some official reactions. For instance, the European Commission issued a [Statement](#) on 6 October, which aims to send a message of calm and which states that it is working towards providing clear guidance to national authorities on how to address data flows to the US in order to make sure that the answers provided by the different Member States are consistent and to provide predictability and legal certainty for citizens and businesses. At the moment, the Commission suggests that businesses base their data transfers on other legitimate grounds as set out in the applicable regulations. Conversely, the SDPA has issued a brief [press release](#) summarising the judgment, but practical questions have not been addressed yet. In any

case, we must keep an eye out on what the national authorities (in particular, the SDPA) may say in the near future either directly or through forums such as the Article 29 Working Party, and on the reaction of the European institutions.

The judgment is expected to speed up the negotiations on the Safe Harbor agreement that began in November 2013 and on which total consensus has not yet reached. In particular, according to reports, it is because of some relevant matters that were also underlined in the judgment of 6 October 2015 (such as access to data by the US public authorities) that the parties have not yet executed the new safe harbor agreement.

WILL THIS JUDGMENT AFFECT TO THE FUTURE EUROPEAN DATA PROTECTION REGULATION?

The Council, the European Commission and the European Parliament are currently discussing the draft Regulations. The negotiations regarding the regulation of international transfers have not concluded yet and, therefore, it is likely that this judgment and the guarantees required for the processing of data of European citizens abroad will have a bearing on the final wording of these Regulations.



Leticia López-Lapuente

Counsel. Madrid office

leticia.lopez-lapuente@uria.com / +34915860131



Reyes Bermejo Bosch

Senior associate. Madrid and Valencia offices

reyes.bermejo@uria.com / +34915860131