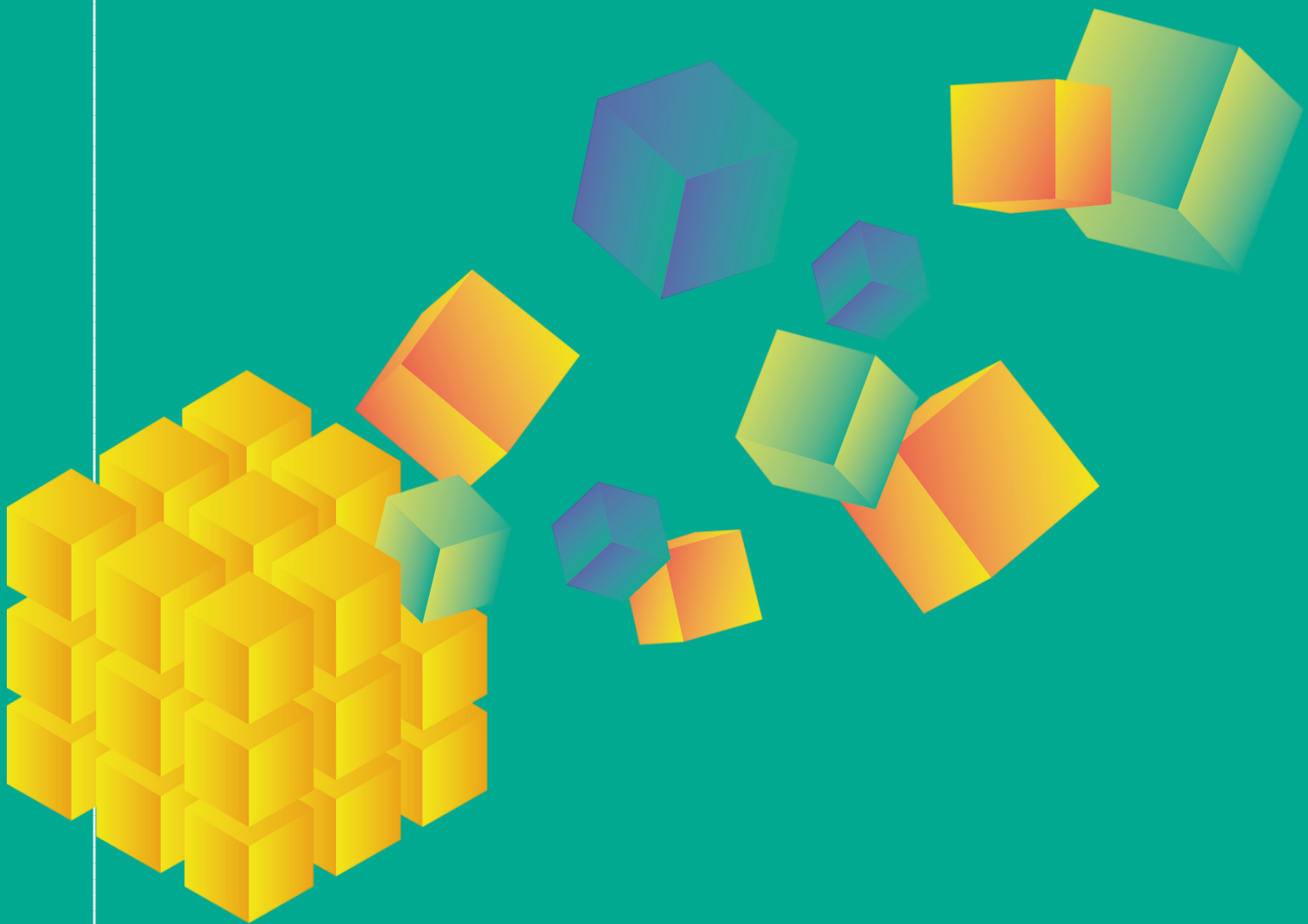


# DATA PROTECTION

Abolishment of the Privacy Shield: How to safely transfer data outside EU?



## → Abolishment of the Privacy Shield

---

### How to safely transfer data outside EU?

With the judgment of 16 July 2020, the Court of Justice of the European Union ("CJEU") declared invalid the EU Decision 2016/1250 of the Commission which established the adequacy of the Privacy Shield: i.e., the legal instrument that allowed the transfers of personal data from the European Union to the USA until a few months ago. This is five years after the decision that had invalidated the forerunner of the Privacy Shield, the "Safe Harbor".

In particular, the decision at issue has

- (i) abolished the EU-US Privacy Shield, ruling the unlawfulness of any data transfer to the United States;
- (ii) left unchanged the other alternative legal bases of Articles 46, 47 and 49 of the GDPR which authorise the transfer of personal data outside the EU (including Binding Corporate Rules, consent, legitimate interest);
- (iii) confirmed the validity of the Standard Contractual Clauses adopted by the European Commission, the so-called "SCC".

With specific regard to SCC, i.e. by far the most widely used instrument to justify cross-border transfers, the CJEU has highlighted how they can be an appropriate instrument provided that the countries of destination of the data guarantee a level of protection "substantially equivalent" to that

offered in the EU.

Therefore, 'the data controller established in the EU and the recipient of the transfer of personal data are required to verify, in advance, that the level of protection required by EU law is respected in the third country concerned. The recipient of such a transfer is obliged to inform the data controller of its eventual impossibility to comply with these clauses, in which case it lies under the controller's responsibility to suspend the data transfer and/or terminate the contract'.

This means that the adoption of the Standard Contractual Clauses must necessarily be preceded by an "examination of the degree of protection" offered to data subjects by national legislation and that, where such protection is not adequate to that of the European Union - as is the case in the United States - the signing of the Standard Clauses cannot allow the transfer.

The ruling at issue has given rise to a climate of serious uncertainty for companies, which could be in breach of the GDPR if transferring data to the USA (or other non-statutory states), even if they adopted standard contractual clauses or alternative legal bases. While waiting for the decision of the different countries, we try to stay up to date about further developments.

## → EDPB Recommendations 1/2020

---

### Measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

On 10 November 2020 the European Data Protection Board (EDPB) adopted Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, which will be subject to public consultation until 30 November 2020.

The EDPB clarified that the Recommendations are addressed to data controllers and data processors acting as exporters of personal data outside the European Economic Area ("EEA").

The Recommendations aim at supporting them in

assessing the level of adequacy of other countries and in identifying appropriate measures to guarantee to the transferred personal data the equivalent level of protection that is provided by Regulation (EU) No. 2016/679 ("GDPR"), after the judgment of the Court of Justice of the European Union ("CJEU") in Case C-311/18, Data Protection Commissioner, Facebook Ireland Ltd and Maximilian Schrems ("Schrems II").

Specifically, the EDPB outlines a procedure, divided into different steps, that exporters of personal data must follow before transferring data to other countries.

## MAPPING THE PROCESSING OPERATIONS, WHEN THEY REQUIRE THE TRANSFER OF PERSONAL DATA TO OTHER COUNTRIES

- The EDPB recommends to data controllers and data processors to identify beforehand all processing operations that involve transfers of data outside the EEA, as well as to identify the countries in which the personal data will be processed by the data importer.

- In compliance with the principle of minimization of processing under Article 5.1.c of the GDPR, the personal data transferred must be adequate, relevant and limited to what is necessary for the purposes for which the transfer and processing to the other country takes place.

- This analysis must be carried out before any transfer and, if a transfer of personal data is suspended, the analysis must be updated before resuming the process.

## IDENTIFICATION OF PERSONAL DATA TRANSFER TOOLS

- First of all, it is necessary to verify that the instrument on which the transfer of personal data to other countries is based falls within the scope of Chapter V of the GDPR.

- If the transfer is to take place to a country for which the Commission has published an adequacy decision under Article 45 of the GDPR, no further measures need to be taken. However, adequacy decisions do not prevent either the data subject from lodging complaints, or the supervisory authorities from bringing a case before a national court when doubts on the validity of a decision arise. In this way the national court can refer a preliminary ruling to the CJEU on the validity of the decision.

- In case of absence of an adequacy decision, the transfer may be made using one of the instruments indicated in Art. 46 of the GDPR (including the Standard Contract Clauses and the Binding Corporate Rules) or, if the conditions are met, using one of the exceptions provided by Art. 49 of the GDPR (including the explicit consent of the data subject; necessary transfer for the conclusion or execution of a contract concluded between the data controller and another natural or legal person in favour of the data subject; transfer necessary to ascertain, exercise or defend a right in court).

- If a transfer tool pursuant to Article 46 of the GDPR is used, it must be ensured that personal data will benefit in the country of destination of a level of protection substantially equivalent to that guaranteed by the GDPR.

- Furthermore, when the transfer takes place under one of the exceptions provided by Article 49 of the GDPR, it must be taken into account that Article 49 is of an exceptional nature and the exceptions it contains must be interpreted restrictively (as indicated in the Guidelines 2/2018 on exceptions under Article 49 of Regulation 2016/679, adopted by the EDPB on 25 May 2018) and refer mainly to occasional and non-repetitive processing activities.

## ASSESSMENT OF THE LEVEL OF PROTECTION OFFERED BY THE COUNTRY OF DESTINATION

- The EDPB recommends assessing, possibly in cooperation with the data importer, whether there are legal rules or practices in the third country that may affect the effectiveness of the safeguards provided by the chosen transfer tool, in the light of the context in which the transfer of personal data takes place.

- The relevant rules of law or practice in the third country should be identified according to the circumstances characterizing each transfer, i.e:

- (i) the purposes for which personal data are transferred and processed (e.g. marketing, HR, IT support, clinical trials),
- (ii) the type of entities involved in the transfer (e.g. public or private entities),
- (iii) the sector within which the transfer takes place,
- (iv) the categories of personal data transferred,
- (v) whether personal data will be stored in the third country or there will only be remote access to data stored within the EEA,
- (vi) the format of the data to be transferred (clear, pseudonymized or encrypted),
- (vii) the possibility of data being subject to onward transfers, within the same third country or to other third countries.

- Particular attention should be paid to laws setting out the requirements for the disclosure of personal data to public authorities or the granting of powers of access to such data.

- European Union rules, such as Articles 47 and 52 of the Charter of Fundamental Rights of the European Union, should be used as a reference to assess whether such power of access by public authorities is limited to what is necessary and proportionate in a democratic society and whether data subjects are granted an effective way to lodge the complaint.

- Attachment 3 identifies an illustrative list of sources to be used to complete the above assessment.

## IDENTIFICATION AND ADOPTION OF ADDITIONAL MEASURES

- If the assessment referred to in point 3 above has shown that the chosen transfer tool is not effective, the EDPB recommends to consider, also in cooperation with the data importer, whether additional measures can provide a level of protection for personal data that is broadly equivalent to that guaranteed by the GDPR.

- Such measures should be identified on a case-by-case basis and may consist of technical, contractual or organisational measures, which may need to be combined. Attachment 2 contains an illustrative list of additional measures (including encryption or pseudonymisation of personal data to be stored in the third country, without communication to the data importer of the decryption or re-identification key; contractual obligations to provide information on access requests by the public authorities of the third country; strengthening of control and monitoring powers by the data exporter, appointment of an intra-group team dedicated to the management of issues related to the transfer of data to third countries).

- A number of factors must be taken into account by the data exporter when identifying the most effective additional measures to protect the transferred data, i.e: (i) the format of the data to be transferred (unencrypted, pseudonymised or encrypted), (ii) the nature of the data, (iii) the complexity of the processing flows, (iv) the number of parties involved in the processing and the relationship between them, (v) the possibility of onward transfers of data within the same third country or to other third countries.

- Where the data exporter concludes that, given the circumstances of the transfer and any additional measures, it is not possible to provide adequate safeguards for the personal data, the transfer must not be started or must be interrupted. In this case, personal data already transferred must be returned or deleted. If, despite this conclusion, it is still intended to transfer the data, a communication must be sent to the competent national authority.

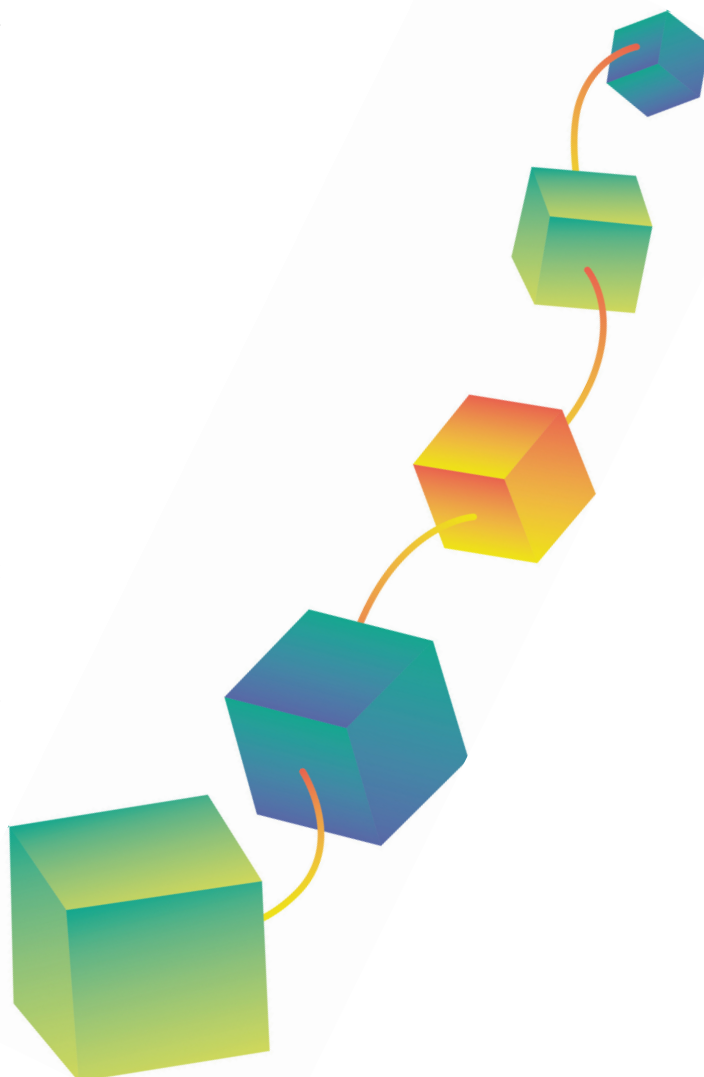
## COMPLIANCE WITH ANY FORMAL PROCEDURES FOR TAKING ADDITIONAL MEASURES

- If additional measures to those provided by the Standard Contractual Clauses are to be taken, it is not necessary to request ad hoc authorization from the supervisory authority, provided that the additional measures identified do not directly or indirectly contradict the Standard Contractual Clauses and are sufficient to ensure a level of protection equivalent to that guaranteed by the GDPR.

## MONITORING AND REASSESSMENT OF THE CHOSEN MEASURES FOR THE TRANSFER OF PERSONAL DATA

- Any developments within the third country to which the personal data are transferred that might influence the initial assessment of the level of protection offered, should be monitored on an ongoing basis, also in cooperation with the data importer.

- To this purpose, the EDPB recommends that appropriate mechanisms should be put in place to ensure the suspension or termination of transfers where the data subject has breached or is unable to comply with the commitments or where additional measures are no longer effective within the third country.



## CONTACT DETAILS

### CZECH REPUBLIC



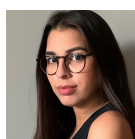
MONIKA GARDLÍKOVÁ  
Attorney-at-law  
Associate  
T +420 236 163 710  
monika.gardlikova@roedl.com

### LATVIA



ANNA KUŠNERE  
Attorney-at-law  
Certified Data Protection Specialist  
+371 (67) 338 - 125  
anna.kusnere@roedl.com

### ESTONIA



DANA IHSANOVA  
Attorney-at-law  
Jurist  
T +372 6068 650  
dana.ihsanova@roedl.com

### LITHUANIA



JŪRATĖ MASIULYTĖ-KATAKINĖ  
Attorney-at-law  
Senior Associate  
T +370 5 2123 590  
jurate.masiulyte@roedl.com

### FINLAND



PEKKA PULLI  
Attorney-at-law  
Partner  
T +358 (09) 696 222 11  
pekka.pulli@roedl.com

### POLAND



GRZEGORZ GĘBOREK  
Attorney-at-law  
Senior Associate  
T +48 32 330 12 00  
grzegorz.geborek@roedl.com

### FRANCE



LEILA BENAÏSSA  
Attorney-at-law  
Senior Associate  
T +33 1 56 92 39 14  
leila.benaissa@roedl-avocats.fr

### SPAIN



JORGE GONZÁLEZ  
Attorney-at-law  
Associate  
T +34 91 535 99 77  
jorge.gonzalez@roedl.com

### GERMANY



ALEXANDER VON CHRZANOWSKI  
Attorney-at-law  
Associate Partner  
T +49 3641 403 530  
alexander.chrzanowski@roedl.com

### TURKEY



EKIN DILEK  
Attorney-at-law  
Partner  
+39 02 6328841  
ekin.dilek@roedl.com

### ITALY



NADIA MARTINI  
Attorney-at-law  
Partner  
T +39 02 6328841  
nadia.martini@roedl.com

### UK



KIRAN MUNAWAR  
Solicitor  
Associate  
T +44 (0) 121 227 8963  
kiran.munawar@roedl.com

## Subscribe to our newsletter! Data Protection Bites – Highlights from all over the world

Our international newsletter aims at collecting all updates, news and insights on data protection issues, with particular attention to the GDPR.

[Read more »](#)  
[Subscribe for free »](#)

[Click here to read the privacy policy](#)

Follow us on



This newsletter is not intended to provide legal advice. No legal business decision should be based on this information. In case of any questions regarding its contents, please contact your Rödl & Partner contact person or write an email to [comunicazione@roedl.it](mailto:comunicazione@roedl.it).

The information and assessments contained therein are of a general nature, do not constitute legal or tax advice, nor exhaustive examination of the topics dealt with, as they cannot replace or be construed as customized legal or tax advice services that we recommend requesting where you are interested in the analysis and processing of concrete questions and cases.

The entire content of the investigation constitutes the intellectual property of Rödl & Partner and is protected by copyright. It is permitted to download, print or copy the details exclusively for personal use. Any modification, copying, disclosure or free reproduction of the contents or parts thereof, whether online or offline, require prior written permission from Rödl & Partner.