
# Transfer of personal data to third countries: clarifications and new measures after the “Schrems II” judgement

# Table of Contents

MORRI ROSSETTI

# The “Schrems II” judgement of the CJEU

# The "Schrems II" judgement of the CJEU

## The CJEU's judgement

MORRI ROSSETTI

In its decision published on 16 July 2020 (the so-called "**Schrems II**"), the Court of Justice of the European Union ("**CJEU**") has **invalidated** the **Decision** 2016/1250 adopted by the European Commission ("**EU Commission**") pursuant to art. 45 of the Regulation (EU) 2016/679 "*on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*" ("**Regulation**" or "**GDPR**") on the **adequacy** of the protection provided by the EU-US Privacy Shield.

The invalidity is due to the USA domestic law that allows public authorities to access - for national security purposes - to personal data transferred from the European Union ("**Union**" or "**EU**").

In particular, the CJEU considered that such legislation:

- ✗ by limiting the protection of personal data, **it does not meet the requirements of the EU law**;
- ✗ **does not grant data subjects enforceable legal rights against the USA authorities**.

Within the same ruling, the CJEU also examined the EU Commission Decision on Standard Contractual Clauses ("**SCCs**") (*i.e.,* Decision 2010/87 "*on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council*"), considering it **valid**.

In particular, the CJEU ruled that:

- ✓ the mere ground that the SCCs are not binding to the authorities of the third country to which the data may be transferred (being a contractual basis) does not affect the validity of the aforementioned decision;
- ✓ by means of the SCCs, a level of personal data protection substantially equivalent to that guaranteed by the GDPR within the EU must be ensured;
- ✗ if the SCCs are breached or it is impossible to comply with them, the suspension or prohibition of transfers of personal data under the SCCs must be provided.

# Clarifications and new measures after the “Schrems II” judgement

# Clarifications and new measures after the "Schrems II" judgement

MORRI ROSSETTI

## EUROPEAN DATA PROTECTION BOARD ("EDPB")


FAQ "*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 on 23 July 2020 ("**FAQ**").


Task force created during the thirty-seventh plenary session on 2 September 2020.

**Recommendations 01/2020** "*on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" and **Recommendations 02/2020** *"on the European Essential Guarantees for surveillance measures",* published on 11 November 2020 (jointly, "**Recommendations**").

## EU COMMISSION


Draft decision "*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*", published on 12 November 2020.

# EDPB's FAQ

# EDPB's FAQ

## The transfer of personal data to third countries: articles 46 and 49 of the GDPR

MORRI ROSSETTI

No grace period is provided to continue transferring data to the United States on the basis of the Privacy Shield and therefore any transfer of personal data based on it is, to date, **illegal**.

Nevertheless, organisations may transfer personal data to the USA and, in general, to third countries by adopting the other mechanisms provided for in the Regulation:

### art. 46 of the GDPR

A data controller (or a data processor) may transfer personal data to a third country (or an international organisation) "***only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available***", including- *inter alia* – SCCs and *Binding Corporate Rules* ("**BCRs**").

### art. 49 of the GDPR

In the absence of an adequacy decision or of appropriate safeguards, a transfer of personal data outside the EU shall take place only if at least one of the conditions set out in art. 49, par. 1, GDPR is met.

! The FAQ are available at the following link: edpb.europa.eu/our-work-tools

# EDPB's FAQ
## SCCs and BCRs

MORRI ROSSETTI

**SCCs and BCRs may be compliant with applicable data protection law under the following conditions:**

1. the data exporter (*i.e.*, a data controller or processor who transfers personal data) has assessed all the **circumstances of the transfer**, including the legislation of the third country of destination enabling or not the data importer (*i.e.,* a data processor or controller who receives personal data) to **comply with the obligations provided for in the SCCs or BCRs**;

2. **supplementary measures to be applied to the processing of personal data** are defined (*i.e.*, encryption systems in which only the data exporter has the decryption key and anonymisation or pseudonymisation systems that allow only the data exporter to identify the data subjects);

3. a case-by-case **analysis of the circumstances surrounding the transfer is carried out in order to ensure that an adequate level of protection pursuant to GDPR** is guaranteed. Should the outcome be negative, it will be necessary:
   - to suspend or terminate the transfer of personal data; or
   - whether the transfer of data is to continue despite this conclusion, to inform the competent supervisory authority (in Italy, the "*Autorità garante per la protezione dei dati personali*").

# EDPB's
## Derogations pursuant to art. 49 of the GDPR

MORRI ROSSETTI


**The EDPB has provided clarifications regarding the following cases in which - in the absence of an adequacy decision or appropriate safeguards - the transfer of personal data outside the EU is authorised pursuant to art. 49, par. 1, GDPR:**

### Consent of the data subject

The consent shall be:

- ✓ **explicit**;
- ✓ **specific** for the particular data transfer, meaning that the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made;
- ✓ **informed**, particularly as to the possible risks of the transfer resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented.

### Performance of a contract

With regard to transfers necessary for the performance of a contract between the data subject and the controller, it should be borne in mind that the transfer must be:

- ✓ **objectively necessary for the performance of the contract**;
- ✓ **occassional**.

### Public interest

In relation to transfers necessary for reasons of **public interest**, it should be borne in mind that:

- ✓ public interest has to be **important**;
- ✓ data transfers **can not take place on a large scale and in a systematic manner**.

# EDPB's FAQ
## Dealings with data processors

MORRI ROSSETTI


With reference to **transfers made by a data processor appointed pursuant to art. 28, GDPR**, the EDPB has specified that:

the data processing agreement with the data processor pursuant to art. 28, GDPR shall **specify whether or not transfers of data to third countries are authorised** (including those carried out by any sub-processors);

if the data may be transferred to the USA and neither supplementary measures can be provided nor derogations under art. 49, GDPR apply, the only solution is to **negotiate an amendment or supplementary clause to the contract to forbid any transfers outside the EU**;


if the agreement provides that data may be transferred to another third country, it is necessary also to **verify the legislation of that third country to check if it is compliant with the requirements provided for by the GDPR and set out by the CJEU in Schrems II judgment**.

**if no suitable ground for transfers to a third country** can be found, **no transfer of personal data should take place**.

# The task force created by the EDPB

# *The task force created by the EDP*

## The *task force* and the 101 complaints

MORRI ROSSETTI

On 2 September 2020, during its thirty-seventh plenary session, the EDPB has created a taskforce to look into the **101 complaints lodged** - in the aftermath of the CJEU Schrems II judgement - **with EEA Data Protection Authorities against several controllers regarding their use of Google and Facebook services** (*e.g.*, Google Ads e Facebook Connect) which involve the transfer of personal data.


Specifically the complainants - represented by the NGO NOYB - claim that **Google and Facebook transfer personal data to the USA relying on the Privacy Shield (now invalid) or outdated SCCs** and are, therefore, unable to guarantee adequate protection of personal data.

In this respect, the two USA companies have replied that they are guaranteeing the protection of users' data on the basis of the SCCs and that, in any case, they are considering the situation created by the Schrems II judgment.

! For further information, please visit the website available at the following link: edpb.europa.eu/news/

# EDPB’s Recommendations

# EDPB's Recommendations

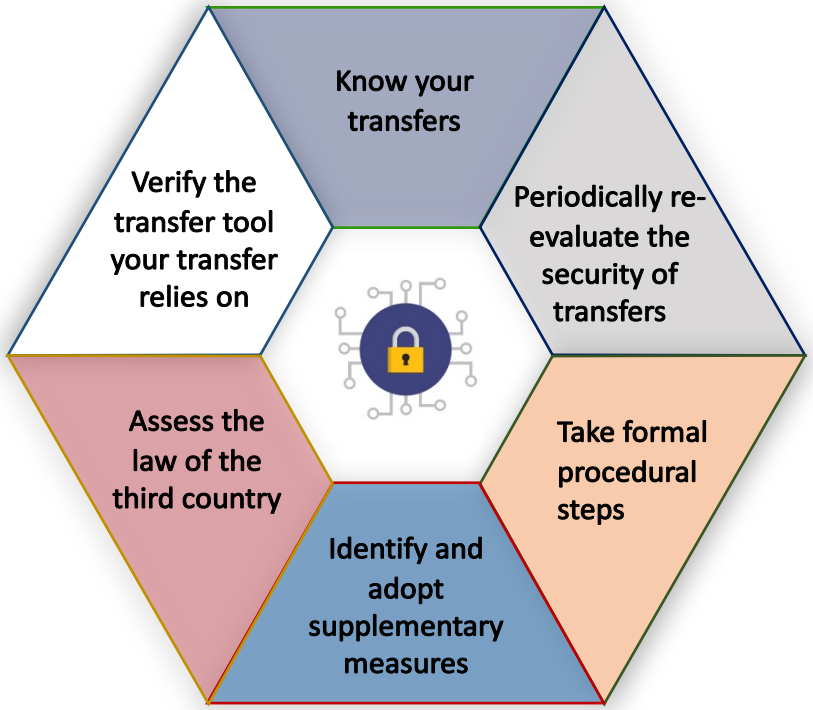
## Recommendations 01/2020 *"on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"*

MORRI ROSSETTI

You must map all transfers of personal data to third countries and verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country.

You must verify the transfer tool your transfer relies on, amongst those listed under Chapter V GDPR.

You must assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer. For evaluating the elements to be taken into account when assessing the law of a third country refer to recommendations 02/2020 (please see the next slide).




You must re-evaluate - at appropriate intervals - the level of protection afforded to the data you transfer to third countries and to monitor if there have been or there will be any developments that may affect it.

You must take any formal procedural steps the adoption of your supplementary measure may require, depending on the art. 46, GDPR transfer tool you are relying on.

You must identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if your assessment reveals that the third country legislation impinges on the effectiveness of the art. 46, GDPR transfer tool you are relying on or you intend to rely on in the context of your transfer.

! The recommendations 01/2020 are available at the following link: edpb.europa.eu/our-work-tools

# EDPB's Recommendations

## Recommendations 02/2020 *"on the European Essential Guarantees for surveillance measures"*

MORRI ROSSETTI

### Clear, precise and accessible rules

The applicable third country law should lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, as well as indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted.

The interference must be foreseeable as to its effect for the individual.

### Necessity and proportionality of the legitimate objectives

The seriousness of the interference should be assessed in the light of the importance of the public interest objective pursued in the third country.

Laws permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.

### Independent oversight mechanism

Any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body.

### Effective remedies for data subjects

Data subject must have an effective remedy to satisfy his/her rights when (s)he considers that they are not or have not been respected in the third country.

! The recommendations 02/2020 are available at the following link: edpb.europa.eu/our-work-tools

# The new EU Commission's SCCs

# The new EU Commission's SCCs
## (1/3)

MORRI ROSSETTI

On 12 November 2020, the EU Commission published a **draft decision on new SCCs** (*i.e.*, "*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*") which will be **available for public consultation until 10 December 2020**.

In this respect, it should be noted that the EU Commission has fixed a grace period of one year from the effective date of the decision, during which data exporters and data importers shall continue to use the SCCs currently approved, implementing, however, supplementary measures ensuring that the transfer of personal data is subject to appropriate safeguards in accordance with art. 46, par. 1, GDPR.

The new SCCs cover the following four types of transfers identified by the EU Commission:

- transfer from **data controller to data controller**;
- transfer from **data controller to data processor**;
- transfer from **data processor to sub-processor**;
- transfer from **data processor to data controller**.

In addition to the general clauses, controllers and processors should select the module applicable to their situation, which makes it possible to tailor their obligations under the SCCs to their corresponding role and responsibilities in relation to the data processing at issue.

In order to provide appropriate safeguards, the SCCs should ensure that the personal data transferred on that basis are afforded **a level of protection essentially equivalent to that which is guaranteed within the EU**.

! The draft decision is available ta the following link: ec.europa.eu/info/law

# The new EU Commission's SCCs
## (2/3)

MORRI ROSSETTI

SCCs shall - *inter alia* - provide:

- the obligation - for the data importer - to **inform** the data controller in the third country if it is unable to follow instructions that would infringe GDPR;
- the obligation – for the data controller - to **refrain** from any actions that would prevent the data processor from fulfilling its obligations under the GDPR;
- **mechanism aimed at assist each other** in responding to inquiries and requests made by data subjects;
- the obligation – for the data importer - to **notify** the data exporter if the data importer is no longer able to fulfil its obligations under the SCCs or is the recipient of a binding order to communicate/make accessible personal data to a public authority;
- **any further measures necessary to comply with the laws in force in the third country and**, in particular**, with any obligations to communicate data to the public authorities** of the third country.

The transfer should **only take place if the laws of the third country of destination do not prevent the data importer from complying with SCCs**.

To that end, they should in particular take into account the specific circumstances of the transfer, such as:

- the **content** and **duration** of the contract;
- the **nature** of the data transferred;
- the **purpose** of the processing;
- any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred.

# The new EU Commission's SCCs
## (3/3)

MORRI ROSSETTI

In addition, in the case of a transfer to a data importer acting as a processor or sub-processor, specific requirements should apply in accordance with art. 28, par. 3, GDPR.

The SCCs should require the data importer to **make available all information necessary to demonstrate compliance with the obligations** set out in the clauses and to allow for and contribute to audits of its processing activities by the data exporter.

**With respect to the engagement of any subprocessor** by the data importer, the **SCCs should in particular set out the procedure for general or specific authorisation** from the data exporter as well as the requirement for a written contract with the sub-processor ensuring the same level of protection as under those SCCs.

With a view to ensuring **transparency of processing**, data subjects should be provided with a copy of the SCCs and should be informed, in particular, of any change of purpose and of the identity of any third party to which the personal data is disclosed.

Lastly, the SCCs should provide for rules on liability between the parties and with respect to data subjects, as well as rules on indemnification between the parties.

Where the data subject suffers material or non-material damage as a consequence of any breach of the third party beneficiary rights under the SCCs, he or she should be entitled to compensation.

This should be without prejudice to any liability under the GDPR.


MORRI
ROSSETTI
OSSERVATORIO
DATA PROTECTION

# Osservatorio Data Protection

MORRI ROSSETTI

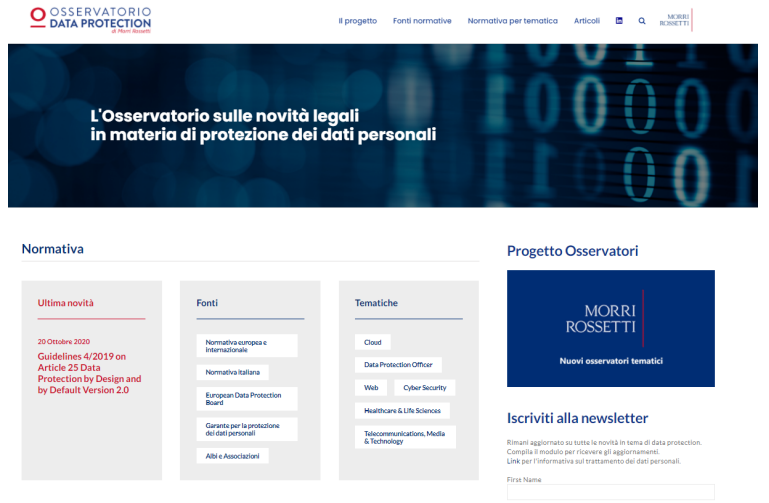
***The "Osservatorio Data Protection" aims to be a useful support and tool in dealing with issues related to the processing and protection of personal data.***

Morri Rossetti's Osservatorio Data Protection, managed by the TMT and Data Protection Team, aims to inform and spread the legal culture within key areas of application of personal data protection legislation.

Over and above a particular attention paid to the healthcare, web, telecommunications, media and new technologies sectors, the project is intended to broaden the scope to other industries highly sensitive to data protection issues. In order to improve the Osservatorio's content, Morri Rossetti collaborates with external professionals specialized in cybersecurity and digital forensics.

**The Osservatorio Data Protection is available at the following link: https://www.osservatorio-dataprotection.it/**

OSSERVATORIO DATA PROTECTION di Morri Rossetti



MORRI ROSSETTI

# Rankings e Credits

# Rankings e Credits

MORRI ROSSETTI

*A renowned quality: Morri Rossetti has received important acknowledgements from first-rate national and international research centres that have certified the high profile of the services our professionals provide to our Clients.*

*«Morri Rossetti is always capable of quickly understanding all the issues related to a deal. The team is always multidisciplinary, composed of tax advisers and lawyers, headed by at least one partner. Their distinctive qualities are the ability to listen and to take care of clients' needs, matched with their technical skills».* The Legal500

*«Their key capabilities compared with other firms are time management, problem solving, attention to details, and the internal organisation between the tax and legal practice areas».* The Legal500

*«We have received a careful, precise and competent assistance that has reserved to the company to correctly frame the problems and to identify the best and most appropriate professional and commercial solutions».* The Legal500

RECOMMENDED Chambers EUROPE 2020 Davide Rossetti

The LEGAL 500 EMEA LEADING FIRM 2020

RANKED IN i migliori studi e professionisti TOPLEGAL guida TAX 2019

TopLegal Industry Awards edizione digitale — FINALISTA 2020 STUDIO DELL'ANNO MEDIA

TopLegal Industry Awards edizione digitale — FINALISTA 2020 STUDIO DELL'ANNO TECHNOLOGY

LEGALCOMMUNITY AWARDS 11.06.2020 — FINALISTA IP&TMT WEB EDITION — IMPALÀ CARLO - MORRI ROSSETTI Avvocato dell'Anno Media e Privacy

LEGALCOMMUNITY AWARDS 11.06.2020 — FINALISTA IP&TMT WEB EDITION — MORRI ROSSETTI Studio dell'Anno Media e Privacy

MORRI ROSSETTI

**Morri Rossetti e Associati**

Piazza Eleonora Duse, 2
20122 Milano (IT)
T +39 02 76 07 971

Info@MorriRossetti.it
MorriRossetti.it