DataGuard

Whitepaper

On the decision of the Court of Justice of the European Union (CJEU, or ECJ)
on July 16, 2020 in the "Schrems II" case

RECOMMENDATIONS FOR THE INTERNATIONAL DATA EXCHANGE

INTRODUCTION

The recent decision on July 16, 2020 by the Court of Justice of the European Union (CJEU), also known as the "Schrems II" case, has far-reaching effects on the international exchange of data, as well as huge implications for businesses. That being said, what exactly are the concrete consequences of the Schrems II decision? What should companies and organisations do to stay compliant in the context of data transfers to the U.S. and the other so-called third countries? What concrete measures should I take as a data processor or controller?

We address these questions in this whitepaper, without claiming to be exhaustive or to propose final answers. The focus is primarily on the expected practical effects as well as practical measures to minimise potential risks. There are of course other interpretations of the judgment and other associated effects - we can already see that with the different published views of the various European data protection authorities on this topic. Nonetheless, we are convinced that we have found a practical and legitimate middle ground to explain the recent developments.

Andreas Rübsam

Computer scientist (FH),
Data protection officer (udisZert),
Head of Privacy (SMB)

Dr. Frank Schemmel

Diploma in Law & Economics, CIPP/E,
CIPM, Data protection officer (TÜV),
Head of Privacy (Corporate)

AT A GLANCE – 11-POINT PLAN TO MINIMISE THE RISKS

The following measures may be considered to reduce possible risks for your company or organisation in connection with the Schrems II decision. We will discuss and describe the individual measures in more detail in a separate chapter below.

01 Checking possible restrictions / terminations of the third country data transfer (especially to the U.S.)

02 Switch from Privacy Shield to SSCs

03 Implementation of additional technical measures prior to third-country transfers (particularly to the U.S.)

04 Instructions and requests to all data importers (especially processors)

05 Instructions and requirements for all processors and sub-processors

06 Additional contractual clauses for service agreements and SCCs

07 Use of the exceptions contained under Art. 49 GDPR

08 Consider alternative providers

09 Review and adaptation of Binding Corporate Rules (BCR)

10 Review and adaptation of the data protection declarations (especially on websites and apps)

11 Update the Records of Processing Activities

WHY DOES SCHREMS II AFFECT MY COMPANY?

Many companies are not aware that the ruling of the CJEU has implications due to globalisation and digitisation. Even if no personal data is actively transmitted to countries outside the European Union (EU) or the European Economic Area (EEA) (countries referred to as "third countries" in data protection), most companies either use service providers, their servers or subcontract with companies in third countries. Therefore, the transfer of data occurs passively or unconsciously.

WHAT IS A DATA TRANSFER?

A data transfer is any processing operation in which personal data are taken outside the scope of the General Data Protection Regulation (GDPR) and to a destination that is outside the EU/ EEA or where data is accessible outside the EU/ EEA. A data transfer can therefore be an active transfer of personal data or simply the accessibility or retrievability from a third country (e.g., for interfaces of service providers to systems or for remote maintenance).

The way of transmission, however, does not matter – it could be done in writing, electronically, orally or by handing over a data carrier.

CAN I SIMPLY TRANSFER DATA ABROAD LIKE THIS?

No, special data protection requirements apply here. The GDPR provides for the transfer of personal data to a country outside the EU / EEA special regulations (Art. 44–49). In general, transfers of personal data to a third country should always be examined with a two-step process:

1. Legal basis: There must be a documented legal basis for the transfer.
2. Adequate level of data protection: Data can only be transferred to a third country if:

- there is an adequate level of data protection as determined by the European Commission; or
- appropriate safeguards have been established according to Article 46 GDPR; or
- a special condition specified under Article 49 GDPR applies.

The GDPR provides the following options for data transfers to third countries:

- **Determination of the adequacy of the data protection level in the third country by the EU Commission (Art. 45 GDPR) – e.g., the one that has now been rejected by the CJEU, the EU and U.S. Privacy Shield. Such adequacy decisions currently exist, among others, for Argentina, Canada, Japan, New Zealand or Switzerland**

- **Availability of appropriate guarantees (Art. 46 GDPR) - e.g., Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs)**

- **Exceptions for certain cases (Art. 49 GDPR) - e.g., Consent, requirement to fulfil a contract or pursuit of legal claims**

WHAT DID THE CJEU EXACTLY DECIDE?

In the "Schrems II" case, the European Court of Justice has ruled on the question of the level of data protection in the U.S. The adequacy decision made by the EU Commission, with the so-called EU and U.S. Privacy Shield, was reviewed and declared null and void. In addition, the question of the validity of Standard Contractual Clauses (SCCs) was considered and ultimately determined as a valid and appropriate guarantee.

WHY IS THE PRIVACY SHIELD NOW INVALID?

The CJEU found that due to the legal access rights of U.S. security authorities to personal data transmitted to the U.S., the U.S. does not have a level of protection comparable to that of the EU. For the people concerned, there are not any sufficient or effective legal remedies available against such infringements. Therefore, the CJEU annulled the Privacy Shield agreement. This annulment applies immediately and without a transition period.

WHAT ARE THE REQUIREMENTS ACCORDING THE CJEU OF DATA TRANSFERRED WITHOUT AN ADEQUACY DECISION?

In the absence of an adequacy decision, in accordance with the requirements of Art. 46.1 GDPR, and according to the CJEU, personal data can now only be transferred to a third country if the data exporter guarantees the following three points:

01	02	03
Suitable guarantees are in place (e.g., SCCs)	**Affected persons are afforded their individual rights**	**Affected persons are provided with effective remedies** (e.g., lawsuit before ordinary courts)

Additional points to consider:

- The contractual arrangement between the data importer in a third country and the data exporter in the EU/EEA
- If necessary, the access to authorities
- The legal system in the relevant third country

MEET THE CURRENT SCHREMS II DECISION ON SCCS

Standard contractual clauses (SCCs) have not been declared fundamentally invalid by the Court of Justice for the European Union (CJEU) and therefore, continue to be a transfer mechanism in some situations. Thus, there are two possible circumstances regarding SCCs.

Circumstance 1:

The appropriate level of data protection can be guaranteed by the data importer based on the SCCs.

Circumstance 2:

The provisions contained in the SCCs are insufficient to guarantee an adequate level of data protection in the relevant third country because of government interference with the rights of data subjects.

WHAT ADDITIONAL MEASURES HAS THE CJEU IMPOSED TO THE DATA EXPORTER AND IMPORTER?

According to the CJEU, the general working of SCCs may, depending on the specific situation of the third country, require additional measures beyond the SCCs to guarantee adequate levels of data protection.

Case-by-case: For this reason, each data exporter must check on a case-by-case basis with the data importer in order to determine:

- whether the SCCs can be used, unchanged, from circumstance 1; or
- whether the legal situation in the relevant third country can provide an adequate level of data protection and if not, additional guarantees beyond the SCCs must be agreed

In concrete steps, this means the following:

01 **Check whether the SCCs can be used unchanged. The following questions must be considered:**

a. Can the recipient of the data in the third country fulfil and guarantee all the SCCs obligations?
b. Is the access by security authorities or other bodies in the third country in question possible?
c. If so, is such access appropriate in principle (suitable and necessary) in order to achieve the targets listed under Art 23.1 GDPR?

02 **Agreement / implementation of additional measures such as:**

a. contractual nature
b. organisational nature
c. technical nature

WHAT ARE THE CONSEQUENCES OF THE SCHREMS II DECISION FOR MY ORGANISATION?

The consequences of the Schrems II decision may be that possible transfers of personal data to countries outside the EU/EEA are no longer permitted under data protection law. Such transfers may be subject to liability, sanctions and reputational risks. Therefore, the following 5 steps must be taken:

1. IDENTIFY AND DOCUMENT ALL THIRD COUNTRY TRANSFERS

Perform a thorough inventory of your organisation's processes/operations and identify all transfers of data to third countries. Do not restrict this process to transfers to the U.S. but also other countries with insufficient data protection levels or insufficient protections of individual rights (e.g. China, India, Russia, Philippines, etc.)

2. IDENTIFY ALL DATA TRANSFERS THAT WERE BASED ON PRIVACY SHIELD

Check which data processing operations with your contractual partners are subject to Privacy Shield and create a corresponding list.

3. IDENTIFY ALL THIRD COUNTRY TRANSFERS THAT ARE BASED ON SCCS

Check which data processing with contractual partners were based on SCCs and create a corresponding list.

4. IDENTIFY THIRD COUNTRIES AND RECIPIENTS WITH CRITICAL DATA PROTECTION STANDARDS

Check and document the existing level of data protection in the recipient country along with the risk and proportionality of government intrusion. It's also important to check the legal system, rights and guarantees in the recipient country and industry.

5. IDENTIFY ADDITIONAL CONTRACTUAL, TECHNICAL AND/ OR ORGANISATION MEASURES FOR SCCS

Identify and implement suitable measures based on the previous risk assessments and contractual, technical and organisational measures to ensure an appropriate level of data protection in the recipient third country. Document these measures in writing and check for compliance or request regular proof of compliance. Document in detail the appropriateness and suitability of the contractually agreed protective measures that have been taken and implemented – the technical and organisational measures, the national legal situation in the third country and why these measures ensure an adequate level of data protection.

WHAT ARE THE AVAILABLE MEASURES TO MITIGATE THE RISK?

DETERMINE IF A RESTRICTION/TERMINATION OF THIRD-COUNTRY TRANSFERS IS POSSIBLE

Check whether it is feasible to stop a transfer to the U.S. and/or other third countries for at least a portion of the personal data records or whether and to what extent, personal data can be processed in a country with an adequate level of data protection.

SWITCH FROM PRIVACY SHIELD TO SCCS

Switch immediately from Privacy Shield to SCCs as the basis of transfer. Immediately conclude corresponding SCCs with your contractual partners. Supplement the SCCs with appropriate guarantees for an adequate level of data protection.

Please see our suggested clauses below. If you need assistance, please reach out to DataGuard at contact@dataguard.com.

IMPLEMENTATION OF ADDITIONAL TECHNICAL MEASURES PRIOR TO THIRD-COUNTRY TRANSFERS (PARTICULARLY TO THE U.S.)

Implement additional technical measures prior to third-country transfers and, for processors such as a U.S.-based cloud service or payment provider. This includes measures such as encryption, pseudonymisation and access restrictions.

The focus should be on minimising the transmission of personal data as much as possible from an organisational or technical point of view. Please make sure that you have the key for encryption in order to carry out asymmetric encryption methods according to the current state of the art, for example, curve 25519, curve 488 or ECC-Brainpool.

Also, check if you can take care of the following:

- That only telemetry data or metadata, excluding personal data, are transferred to a third country, or stored on servers that can be accessed from third countries
- That only necessary website plugins are used. For example, do you prevent the transfer of data to Google through Google Web Fonts by selecting the desired font directly on your server?
- That data on such servers is only stored during the processing and deleted thereafter. Please pay special attention to the storage and deletion of technical data, backups etc.

INSTRUCTIONS AND REQUESTS TO ALL DATA IMPORTERS (ESPECIALLY PROCESSORS)

Promptly ask or request all processors and controllers who have personal data controlled by you to:

a) Inform you whether they are subject to legal requirements which are likely to significantly affect the fulfilment of the guarantees required by the concluded contracts (BCRs, SCCs, etc.).
b) Inform whether and to what extent and on what specific basis (e.g., Freedom Act, Foreign Intelligence Surveillance Act (FISA) 702, U.S. Executive Order 12333, Gramm-Leach-Bliley Act (GLBA), the Dept of Homeland Security Act of 2002, Public Law 110-53), whether within or outside the U.S. they are subject to powers of intervention by U.S. authorities and/or secret services.
c) Confirm that they comply with the measures required by the SCCs and the corresponding level of data protection.
d) Provide appropriately documented information and evidence for point 3.

Unfortunately, the above-mentioned measures are in most cases only theoretical possibilities and due to existing U.S. laws, most likely not fully implementable. However, they will help to reduce your liability risk in your internal relationship with the contractor. If necessary, demonstrate to a regulatory authority that you have taken the necessary steps to avoid violations of data protection law.

INSTRUCTIONS AND REQUIREMENTS FOR ALL PROCESSORS AND SUB-PROCESSORS

a) Instruct all processors who transfer or process personal data to the U.S. under the Privacy Shield to suspend transfers immediately and until your processor or its subcontractor has ensured a level of data protection in accordance with the GDPR on a case-by-case basis. This suspension of data transfers should be officiated in writing or by e-mail.
b) Demand that all processors who transfer or process personal data to the U.S. under the Privacy Shield take all necessary steps (without delay) and at their own expense. This is to establish suitable alternative mechanisms that support a lawful transfer of personal data to the U.S. as soon as possible.

Before you request the suspension of data transfer to the U.S., it is essential that you check the relevant contracts: Do they entitle your contractual partners to termination rights and/or claims for damages? You should also check what effects a suspension of data transmission/ data processing would have on your business. You should also seek advice from your own legal department/external lawyers regarding the consequences of a suspension.

ADDITIONAL CONTRACTUAL CLAUSES FOR SERVICE AGREEMENTS AND SCCS

Ensure that relevant additional contractual obligations and guarantees are included in all current and future service agreements/ SCCs as the current SCCs are, alone, insufficient to ensure an adequate level of data protection in the third country concerned. For this purpose, you can use the following wording, depending on the individual case:

1. *If the Customer or the Contractor invokes a specific legal transfer mechanism for international data transfer in conformity with data protection law and this transfer mechanism is amended, revoked or declared invalid in whole or in part by a competent court, the customer and the contractor agree to cooperate in good faith in order to immediately establish a suitable alternative transfer mechanism to ensure lawful transfer.*

2. *If the Contractor is required by law (e.g. under the Intelligence Surveillance Act (FISA) 702, U.S. Executive Order 12.333, Freedom of Information Act, Gramm-Leach-Bliley Act (GLBA), the Dept of Homeland Security Act of 2002, Public Law 110-53) and/or by order of a court or law enforcement agency, security authority and/or regulatory authority (in particular, but not limited to, the National Security Agency, Homeland Security, Federal Trade Commission) - hereinafter referred to as the „Authorities" to disclose personal data covered by this Agreement, Contractor shall, at its own expense:*

a. Inform the client (to the extent permitted by law) immediately, but at the latest within 24 hours of receipt of the relevant request. The notice should be provided in writing or by e-mail, stating the requested data, the requesting authority, and the legal basis for the requested disclosure; and

b. exhaust all legal remedies available to the Contractor, its affiliated companies and subcontractors in the country concerned through all instances to prevent the disclosure of personal data (in particular, but not exclusively, appropriate proceedings before U.S. District Courts, Circuit Courts, Federal Administrative Courts,

Appellate Courts, Supreme Court), in order to protect the rights and interests of the data subjects under the GDPR and to ensure data processing in compliance with the GDPR; and

c. refrain from disclosing personal data to the above-mentioned authorities until the Contractor, after having fulfilled its above-mentioned obligations, has been ordered by a competent court to disclose the data.

3. *On a regular basis, but at least once per calendar year, the Contractor is obliged to provide the Customer, free of charge, with general information on the requests received from authorities regarding personal data processed under this Agreement (e.g., number of requests for disclosure, type of data requested, requesting party if possible, etc.).*

4. *Contractor shall be responsible for all acts and omissions of its affiliates, employees, agents and subcontractors that violate this section.*

Please consult your legal department/external lawyers to find out whether and to what extent the above obligations or your own suggestions can and should be subject to a contractual penalty at the expense of the contractor.

USE OF THE EXCEPTIONS CONTAINED UNDER ARTICLE 49 GDPR

Check whether the rules for the application of an exception under Art. 49 GDPR are a possible legal basis for the transfer of data to a third country. It should be noted that Art. 49 GDPR is not covered by the European Supervisory Authorities and is a last resort exception for third country data transfers. In principle, such mechanism is designed in a narrow fashion and not meant to be applicable for regular and recurring data transfers (e.g., classic outsourcing scenarios).

Therefore, Art. 49 GDPR should not be a sufficient legal basis for most data transfers.

However, it can be assumed that the European supervisory authorities will have to accept such necessary measures due to the application of Art. 49 GDPR for a temporary transition period.

This will prevent lasting damage to the fundamentally important economic relations between the European Union and the U.S. Despite the aforementioned, a risk remains with the application of such measures.

REVIEWING AND ADJUSTING THE BINDING CORPORATE RULES (BCRS)

The CJEU has put into question the level of data protection in the U.S. As a result, BCRs, like Standard Contractual Clauses (SCCs), are just a contractual construct under private law that has been approved by authorities. The same applies in principle to the transfer of personal data to the U.S. based on BCRs. Whether the BCRs are sufficient to guarantee an adequate level of data protection must be examined on a case-by-case basis and, if not, additional measures may have to be taken. In this context, it is advisable to use clauses and guarantees similar to those for SCCs. Since these adaptations usually involve substantial changes to the BCRs, they would have to be re-submitted to the competent supervisory authority for approval.

REVIEWING AND ADJUSTING THE PRIVACY POLICIES (ESPECIALLY ON WEBSITES AND APPS)

The privacy policy is the "business card of the company" in terms of data protection and should be accessible to every person. In this regard, you should check if your privacy policies on your websites, apps, web stores, etc. list a transfer to a third country and mention the Privacy Shield or SCCs as the transfer mechanism. If they do, such sections may need to be adapted since according to Art. 13 and 14 GDPR, privacy policies are required to reflect the current status of the data processing.

UPDATE OF THE RECORDS OF PROCESS ACTIVITIES

In addition to the privacy policy, the records of processing activities must be updated and adapted accordingly. The records of processing activities are usually requested by supervisory authorities as part of inspections. In addition, the records of processing activities serve as an appropriate source to fulfil inquiries from data subjects (e.g. the right to information according to Art. 15 GDPR). Therefore, the data protection documentation should always be kept up to date.

WHAT ARE THE RECOMMENDATIONS OF THE SUPERVISORY AUTHORITIES?

The opinion of the European supervisory authorities is currently very ambivalent and sometimes even contradictory. For example, while the supervisory authority from the UK, or the Information Commissioner´s Office (ICO), refers to the advice from the European Data Protection Board, it is recommended to conduct a risk assessment to determine whether the SCCs provide enough protection within the local legal framework when the transfer is to the U.S. or another third country. The ICO is taking the time to carefully consider what this means and will continue to apply a risk-based and proportionate approach in accordance with its Regulatory Action Policy.

However, the Berlin supervisory authority has asked all companies under their area of responsibility to stop data transfers to the U.S. and to retrieve the data to Europe or to other countries with an adequate level of data protection. These opposing recommendations are for the practice unsatisfactory and contradict the idea of harmonisation of the GDPR. The European data protection authorities have published an initial FAQ and are currently working on a jointly agreed position regarding concrete measures and recommendations for action.

Below you will find a summary of selected opinions from European Supervisory Authorities:

COLOR SCHEME:

Restrained, neutral or weighed evaluation (no immediate or only little action required)

Strict or restrictive interpretation (clear recommendations for action or information on risks and consequences or sanctions)

Very strict or very restrictive position (clear request to avoid transfers or announcement of reviews or sanctions)

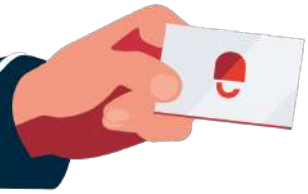
SUPERVISORY AUTHORITY	EVALUATION	OPINION	SOURCE
European Data Protection Board (EDPB)		- In the light of the case law of the European Court of Justice, the EU and the U.S. should create a final and effective framework to ensure the level of data protection for personal data in the U.S. is equivalent to the level of protection in Europe. - SCC are still valid. It is referred to the importance of compliance with the obligations through the data exporter and data importer, especially with what regards the information requirements in case of a change in the legal position of the data importer´s country. - Data exporter and data importer must check together whether in the concerned third country there is an adequate level of data protection, and if not, take appropriate additional action if necessary. The EDPB is still examining how these additional measures can be developed. - Data protection authorities are required to prohibit transfers that violate data protection. - There is no transition/grace period, but the requirements from Schrems II are effective immediately to be implemented.	Press release FAQ

SUPERVISORY AUTHORITY	EVALUATION	OPINION	SOURCE
European Data Protection Supervisor (EDPS)		- It is assumed that the U.S. will do everything in its power to create a legal framework in terms of data protection that meets the requirements of the Court of Justice of the European Union. - EDPS wants to review corresponding contracts of the EU institutions (e.g. with Microsoft).	Press release
Germany – Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI)		- Data transfers to the U.S. via SCCs are still possible but require the completion of additional measures. - The circumstances of data transfers (including to other countries) must be considered on a case-by-case basis and the contracts with appropriate services providers must be checked. - There is no grace period: it must start immediately with the conversion. - Data protection authorities should advise intensively the under their jurisdiction public and private bodies about alternative bases for the international exchange of data and on its implementation.	Press release (24. July) Press release (16. July)
France (CNIL)		- CNIL will follow the reconditioned decision in the European Process the data protection committee (EDPS).	Press release
Ireland (Data Protection Commission)		- It is questionable whether SCC transfers to the U.S. can still be justified. - Regardless of the chosen transfer mechanism, this must achieve a similar European level. - The decision and the consequences as well as any measures to be taken are now being carefully checked by the authority.	Press release

SUPERVISORY AUTHORITY	EVALUATION	OPINION	SOURCE
Netherlands (Autoriteit Persoonsgegevens)		- EU Commission should have taken into consideration a successor agreement for Privacy Shield. - Since there is no equivalent and appropriate level of data protection in the U.S., companies and organisations should no longer transfer personal data to the U.S. - The practical consequences and next steps are to be processed in the European Data Protection Board (EDPB).	Press release
Spain (Agencia Española de Protección de Datos)		- SCC are still valid. - AEPD will follow the decision in Europe prepared by the European Data Protection Board.	Press release
United Kingdom		- Organisations should follow the guidance of the European Data Protection Board, as stated by the ICO. The board recommends conducting a risk assessment as to whether SCCs provide enough protection within the local legal framework, whether the transfer is to the U.S. or elsewhere.	Press release

AND WHAT WILL THE LEGISLATOR DO?

The EU Commission has announced that it will work closely with the U.S. to ensure secure transatlantic data flows. The U.S. has made the same announcement. It is possible to assume that there will be a subsequent agreement to the Privacy Shield (a kind of Privacy Harbour). However, it is not yet possible to estimate when this will happen. After the invalidation of the Safe Harbour in October 2015, it took almost three quarters of a year for Privacy Shield to be negotiated and concluded. Previous experience can serve as a first indication of what the expected time frame for a subsequent agreement will look like.



DataGuard is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalise Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.

Let's talk about your challenges and define first steps on your compliance journey:

Contact us

You might also like:

→ **Data privacy compliant cookie management and tracking**

→ **Guide: Prepare for your GDPR Audit**

→ **Overview of all data privacy documents from the UK GDPR**