Introduction
On July 16th, 2020, the European Court of Justice (CJEU) released its highly anticipated decision in Case C-311/18, otherwise known as Schrems II. The CJEU ruled that the EU-U.S. Privacy Shield is to be invalidated. In turn, the Court ruled that the system of Standard Contractual Clauses (SCCs) which allows for data transfers from the EU to third countries, is valid. While the Court ruled that existing SCCs remain valid, supervisory authorities and data controllers must now assess the situation in the destination country on a transfer-by-transfer basis.

Privacy Shield
The EU-U.S. Privacy Shield is a privacy program for U.S. organizations administered by the U.S. Department of Commerce that previously was an adequacy mechanism that allowed organizations in the EU to transfer personal data to organizations in the U.S. who adhered to the regulatory principles. In the Schrems II case, the CJEU has assessed the validity of the Privacy Shield adequacy decision, and it finds fault with it.

The Two Court Objections
U.S. Government Surveillance:
The problem the Court finds is that the U.S. government surveillance programs run under section 702 FISA, Executive Order 12333 and Presidential Policy Directive 28, are vague. They do not lay down clear and precise rules or impose minimum safeguards to effectively protect personal data against the risk of abuse.

Lack of Effective Redress Where Data Are Subject to Government Surveillance:
Standing case-law in the EU finds that individuals should have the possibility to pursue legal remedies in order to get access to personal data related to them, or to ask for the rectification or erasure of their data. This is especially important when data is being transferred outside of the EU, since authorities cannot protect personal data when it has gone abroad. In this case, the Court found that there are no effective redress mechanisms available for EU data subjects whose data are subject to government surveillance, despite the appointment of a Privacy Shield Ombudsperson.

Standard Contractual Clauses (SCCs)
The Court confirms the use of SCCs should still be possible, although it has tightened the rules for the use of SCCs quite a bit. A data exporter and data importer must assess whether they believe they can meet the requirements of the SCCs in their specific situation. The data exporter and data importer will need to undertake an assessment of the law of the country where data is flowing to, including an assessment of any national security legislation. Without such an assessment, agreeing on the adequate safeguards would not be possible.

What's Next
At the time of writing, the verdict of the CJEU leaves data transfers from the EU to the U.S. in limbo for now. It is clear the Privacy Shield can no longer be used, but a lot of questions remain as to whether SCCs remain valid for data transfers between the EU and the U.S., or other countries with impactful national surveillance systems for that matter. U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders have released a joint statement indicating that discussions have been begun to evaluate an enhanced version of the EU-U.S. Privacy Shield.
Table of Contents

Privacy Shield

What do I need to do about my current Privacy Shield self-certification?
I want to withdraw EU-US from Privacy Shield. What do I need to do?
Are prior data transfers under EU-US Privacy Shield affected?
Will there be a grace period?
Should I update my Privacy Notice?
Will there be a replacement for Privacy Shield?
Has the Swiss-US Privacy Shield been invalidated?
The Department of Commerce has stated that it will continue to operate the Privacy Shield. What is the benefit of continued participation?
What about onward transfers of data from U.S.-based companies processing EU personal data to other U.S.-based companies (e.g. cloud providers)?

European Regulator Views

What have the European regulators and authorities said about the decision and Privacy Shield?
What impact will these developments have on Brexit and the U.K?

National Security Considerations

What is the best way to determine if a company is subject to National Security laws?
What is your recommendation if one of your sub processors is subject to FISA 702, EO 12333, or PPD 28?

GDPR Compliance and Fines

What GDPR responsibilities does this decision affect?
What are the fines for non-compliance with the data transfer requirements of GDPR?
Standard Contractual Clauses

Can I transfer personal data from the EU to the U.S. under SCCs?

Can I transfer personal data from the EU to other countries under SCCs?

Would strong encryption be a sufficient mitigating measure for the potential interference of U.S. surveillance laws?

What assessment criteria should I consider for whether the data importer can meet its obligations under the SCCs?

If my organization has EU data stored by a cloud service provider in the U.S. can SCCs still be relied upon? Do I need to demonstrate that the data is of no known national security significance?

If my organization signs a Data Processing Agreement in combination with existing SCCs, is that enough protection to transfer personal data from the EU?

Other Transfer Mechanisms

Are the other transfer methods still valid for transferring data?

To what extent does the CJEU decision limit the use of explicit consent (art. 49(1)) for the transfer of personal data to the U.S. (or elsewhere)?

Do the data transfer requirements apply to data backups that are taken and stored in another region?

If my U.S. business shifts server or data location to the EU do I still have a need for a data transfer mechanism?

Isn't this EU Court decision flawed because EU citizens cannot exercise their rights as it relates to National Security within the EU either?

I am relying on BCRs for my data transfers. Is there any guidance available?
Privacy Shield

What do I need to do about my current Privacy Shield self-certification?

The U.S. Department of Commerce (DOC) has stated that it will continue to operate Privacy Shield and it expects participants to continue to uphold their Privacy Shield obligations. The U.S. DOC, European Commission, and European Data Protection Board all have indicated that they intend to create a successor to Privacy Shield and the European Commission and DOC have initiated discussions. Remaining in Privacy Shield may simplify your transition to a successor arrangement between the EU and the U.S. At this time, you are required to continue to uphold your Privacy Shield protections for data you have collected pursuant to Privacy Shield. You do need to ensure an alternative mechanism to transfer personal data from the EU to the U.S., since Privacy Shield can no longer be used to do so.

I want to withdraw EU-US from Privacy Shield. What do I need to do?

If you decide to withdraw from Privacy Shield, you need to follow the process established by the U.S. Department of Commerce. If you withdraw, we have developed an alternative International Privacy Verification Program to enable you to continue to demonstrate that you are continuing to protect the data received pursuant to Privacy Shield. If you choose to withdraw, we will provide more guidance on how you can transition over to that program, or an alternative program of your choice.

Are prior data transfers under EU-US Privacy Shield affected?

All prior data transfers remain subject to the obligations of Privacy Shield.

Will there be a grace period?

EDPB has released guidance stating that there will be no grace period. Given that the Privacy Shield has been invalidated by the Court, companies that used the Shield so far for EU-U.S. data transfers will need to find an alternative legal basis for the transfer without undue delay.

Should I update my Privacy Notice?

We recommend that you do not make any changes to your Privacy Notice as a Privacy Shield participant at this time. There is no basis or regulatory guidance for making any changes to your Privacy Notice at this time unless you have stated (as a data exporter under GDPR) that you rely on Privacy Shield as a legal basis for data transfer from the EEA.

My organization’s Privacy Policy clearly states that we use Privacy Shield to legitimize our data transfers from EU to U.S., should we remove this notice?

Recognizably, there is no easy way to address this. You will need to update your notices, ideally you would be able to state what alternative you are using. Other organizations may consider including a placeholder that states the organization is reviewing the Schrems-II decision.

Will there be a replacement for Privacy Shield?

We expect a replacement for Privacy Shield to be negotiated between the EU Commission, the EU Member States and the U.S. Government. On August 10, 2020 the DOC and the European Commission released a statement indicating they have initiated discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework. At this time, no details on timeline or scope are available. Based on the CJEU decision, if
changes are not made to U.S. law, it is possible that a replacement arrangement may have a more limited scope to organizations that are not subject to national security surveillance program requests.

Has the Swiss-US Privacy Shield been invalidated?
No. However, as of 8 September 2020, the Swiss Federal Data Protection Authority has decided the Swiss-U.S. Privacy Shield no longer offers adequate safeguards for the protection of personal data. This means the Swiss-U.S. Privacy Shield can not be used any longer for cross-border data transfers from Switzerland to the U.S. Companies that have used the Swiss-U.S. Privacy Shield until now, will need to start using alternative data transfer mechanisms.

The Department of Commerce has stated that it will continue to operate the Privacy Shield. Is there a benefit of continued participation?
The U.S. DOC, European Commission, and European Data Protection Board all have indicated that they intend to create a successor to Privacy Shield. Additionally, the European Commission and DOC have initiated discussions. Remaining in Privacy Shield may simplify your transition to a successor arrangement between the EU and the U.S. At this time, you also are required to continue to uphold your Privacy Shield protections for data you have collected pursuant to Privacy Shield. Remaining in Privacy Shield will simplify these processes for your organization and, depending upon how you have structured your privacy program, may also help your organization comply with other international data transfer commitments, such as those you would need to make if you are able to enter into SCCs for data transfers you receive.

What about onward transfers of data from U.S.-based companies processing EU personal data to other U.S.-based companies (e.g. cloud providers)?
Also onward transfers or personal data originating from any of the EEA countries, need to be processed in accordance with the data protection standards set by the GDPR. The data exporter is responsible for the full chain of processing of data for which they are the data controller. If the data importer, or their service providers, cannot guarantee that the safeguards included in the GDPR and the applicable transfer mechanisms can be met, additional safeguards need to be agreed. If this is not possible, the data transfer cannot take place. In their FAQs, the EDPB recommends companies to verify the language in their data processing agreements.
European Regulator Views

What have the European regulators and authorities said about the decision and Privacy Shield?

Various authorities have provided guidance or statements on the decision including specifics regarding data transfers under Privacy Shield. Visit our website’s Resources page to read the latest regulator guidance. On 24 July, the EDPB released a first version of a FAQ document, providing initial answers on the Schrems-II fallout. A joint press statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders was issued on August 10.

What impact will these developments have on Brexit and the U.K.?

It is too early to tell. Until the end of the transition period (for now until 31 December 2020), the U.K. will continue to apply the GDPR without change. What will happen next is subject to negotiations between the U.K. government and the European Commission. What is clear, is that the “essentially equivalent” standard to assess a third country’s legal framework for data protection, will also need to apply when assessing the U.K. in order to decide on adequacy.

National Security Considerations

What is the best way to determine if a company is subject to National Security laws?

The best way is to ask your data importer because they should have a good idea of what legislation they are required to adhere to within the country they operate within.

What is your recommendation if one of your sub processors is subject to FISA 702, EO 12333, or PPD 28?

There is no easy solution for the moment. One of the considerations could be to (temporarily) ensure all data originating from Europe is stored on European servers, to limit the amount of data transfers taking place. For clarity: also accessing personal data from a computer in the U.S. is considered a processing operation, and thus...
constitutes a data transfer if the data is stored in Europe.

**GDPR Compliance and Fines**

**What GDPR responsibilities does this decision affect?**

The decision relates to the responsibilities of data controllers and processors based in the EEA for the transfer of data to countries outside the EEA. Any such transfers need to ensure the level of protection offered to the data is not undermined by the transfer, and thus requires the use of a “transfer mechanism”. These are:

- **Adequacy**: an adequacy decision allows for unlimited data transfers to the country, region or sector that has received such a decision approved by the European Commission, following advice from the EDPB and the EU Member States. The countries with an adequacy decision are Andorra, Argentina, Canada (only under PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. All adequacy decisions are currently under review following the entry into force of GDPR.

- **Appropriate Safeguards**: The GDPR allows for contractual safeguards to be agreed between the data exporter and the data importer, that guarantee the personal data are well protected. Following Schrems-II, this means a level of protection that is “essentially equivalent” to the GDPR. Contracts may use so-called Standard Contractual Clauses (or Model Clauses) approved by the European Commission or by national data protection authorities (both in cooperation with the EDPB). Companies can also use a custom contract, which is subject to DPA approval before it can be executed.

- **Binding Corporate Rules**: The GDPR allows for intra-group contractual safeguards to be agreed between the entities of a multinational group of companies and their lead DPA. Such BCRs are subject to approval by the EDPB. Following the Schrems-II decision, also BCRs need to ensure an “essentially equivalent” level of data protection in light of GDPR.

- **Derogations**: The GDPR provides for derogations in Article 49, which may include contracts or consent. The EU DPAs have made clear these derogations need to be used restrictively, meaning they cannot be used for continuous, structural or massive data transfers. They reason the exception cannot become the rule for international transfers.

The CJEU has made clear that if the data exporter and data importer cannot guarantee that the safeguards of the GDPR can continue to apply in a third country, for example because the third country has surveillance legislation which is not restricted to what is strictly necessary from an EU perspective (meaning the surveillance should be based on clear, precise and accessible rules, should be proportionate, and should include both independent oversight and effective (judicial) remedies for the individual, as explained by the WP29), the data transfer cannot take place and needs to be stopped. DPAs are required to end the data transfer as well if they come across such data transfers during an investigation.

**What are the fines and penalties for non-compliance with the data transfer requirements of GDPR?**

Up to 4% of annual revenue or 20 M EUR, whichever is higher. Additionally, the DPAs have the power to issue a decision to suspend the data transfers from their country to the U.S.
Standard Contractual Clauses

Can I transfer personal data from the EU to the U.S. under SCCs?

As long as the data are not subject to collection and/or access by U.S. authorities for national security purposes, SCCs can be used on a case-by-case basis subject to assessment of whether the U.S. data importer can meet its SCC obligations for the specific data processing. This means the burden of proof on both the data exporter and the data importer in the third country, has increased, to verify they can meet all the requirements of the SCCs. The data importer will also need to confirm that they will fully respect all the core principles under GDPR. It also means that the data importer and exporter will need to assess the legislation of the third country to see if for example they are subject to surveillance laws which may cause an interference of the supplemental rights. If that is the case, then the transfer cannot take place based on SCCs. This is similarly applied to Binding Corporate Rules (BCRs).

In their FAQ document, the EDPB has indicated it will provide further guidance on the legal, technical and organisational measures that could be taken to supplement SCCs to ensure a continued legal data transfer.

Can I transfer personal data from the EU to other countries under SCCs?

As long as the data are not subject to access by government authorities for mass surveillance or other data processing programs without strict limitations, SCCs can be used on a case-by-case basis subject to a documented assessment of whether the data importer in the third country can meet its SCC obligations for the specific data processing. In particular, third countries where there may be significant concerns due to mass surveillance projects in place include: Australia, Canada, China, India, Israel, New Zealand, Russia, Switzerland, and the United Kingdom. [Note, due to the structure of GDPR, assessment of intra-EEA transfers is not required]

In their FAQ document, the EDPB has indicated it will provide further guidance on the legal, technical and organisational measures that could be taken to supplement SCCs to ensure a continued legal data transfer.

Would strong encryption be a sufficient mitigating measure for the potential interference of U.S. surveillance laws?

Encryption is a good security mechanism that means the data cannot be intercepted. However, there are other mechanisms that may allow for the U.S. government to access personal information. Ultimately the data set could be decrypted when accessed by other parties.

What assessment criteria should I consider for whether the data importer can meet its obligations under the SCCs?

(a) Is the data importer a provider of services that facilitate communications or electronic interactions between individuals, e.g., an Internet Service Provider or electronic communication services provider?

(b) Has the data importer ever been subject to a data access request for national security purposes?

(c) Has the data importer ever been subject to a data retention request for national security purposes? If the answer is “yes” to any of these, and the data importer is not in a country recognized by the EU as providing “adequate protection,” then SCCs are unlikely to be a valid transfer option in the absence of express authorization from the DPA in the originating country. If, “no,” proceed with a third party risk assessment to evaluate effectiveness of the importer’s controls.
If my organization has EU data stored by a cloud service provider in the U.S. can SCCs still be relied upon? Do I need to demonstrate that the data is of no known national security significance?

If your subprocessor (e.g. a cloud service provider) is subject to those national security laws then there might be a challenge from the Schrems-II perspective because in the end as the data controller (exporter) you remain responsible for international data transfers and the data that you have collected. Your organization must ensure that protection remains in place as the data travels. The EDPB recommends to at least verify the contractual language in your data processing agreement, in order to verify whether third country data transfers are allowed in the first place, also when using sub-processors, and to adduce additional safeguards where relevant.

If my organization signs a Data Processing Agreement in combination with existing SCCs, is that enough protection to transfer personal data from the EU?

No, based on the CJEU’s Decision and guidance from the EDPB, a case-by-case assessment is needed prior to determining whether a DPA in combination with SCCs would be sufficient for the specific transfer.
Other Transfer Mechanisms

Are the other transfer methods still valid for transferring data?

All data transfer mechanisms included in the GDPR have remained valid. The CJEU has invalidated one of the adequacy decisions (for the Privacy Shield) and has set stricter assessment criteria for the use of the other transfer mechanisms.

I am relying on BCRs for my data transfers. Is there any guidance available?

In BCR approvals adopted following the Schrems-II judgment, the European Data Protection Board has added a specific disclaimer related to the now required case-by-case assessments:

“In accordance with the judgment of the Court of Justice of the European Union C-311/187, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, [Company Name] and its Group Companies should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.”

To what extent does the CJEU decision limit the use of explicit consent (art. 49(1)) for the transfer of personal data to the U.S. (or elsewhere)?

The CJEU decision has not limited the use of consent for the transfer of personal data. On the contrary - the Court mentions consent as one of the options to transfer personal data, which means there is not a legal vacuum. Companies should be aware however, that in the EDPB guidance on the use of the derogations under Article 49 GDPR, it is made clear these cannot be used for continuous, structural or massive data transfers.

Do the data transfer requirements apply to data backups that are taken and stored in another region?

Yes. Neither the GDPR, nor the Court, makes any reference to exceptions that would exist for archiving purposes, for scientific or historical research purposes or for statistical purposes.

If my U.S. business shifts server or data location to the EU do I still have a need for a data transfer mechanism?

That depends on how the data is being processed within the company. As long as the data is stored on servers in the EEA and only accessed from within the EEA, no data transfer mechanisms will be needed. However, as soon as access to the data is made from outside the EEA countries, a data processing operation is taking place (according to the definition of Article 4(2) GDPR), which would also constitute a data transfer, thus requiring the use of a transfer mechanism. In addition, if the company is subject to U.S. surveillance legislation, including but not limited to Section 702 FISA and E.O. 12333, using an EU server is not a guaranteed protection. Both have a broad scope, that allow the U.S. intelligence and security services to also collect data outside the U.S. territory.
Isn’t this EU Court decision flawed because EU citizens cannot exercise their rights as it relates to National Security within the EU either?

First of all, it is important to understand the European Union has no competence as regards the national security of the Member States. The Court therefore is not allowed to assess whether Member States’ surveillance laws would be in line with the EU Charter on Fundamental Rights. However, all EU Member States have also signed the European Convention on Human Rights, and are therefore subject to the oversight by the European Court of Human Rights in Strasbourg, that is in most situations allowed to assess surveillance laws against fundamental rights requirements. The Court has also done so in the past, as is clear from the WP29 assessment.

From a study completed by the EU Fundamental Rights Agency, it can be understood that most Member States indeed do have surveillance laws, but also have put in place processes for individuals (irrespective of nationality) to exercise their rights.

I am relying on BCRs for my data transfers. Is there any guidance available?

In BCR approvals adopted following the Schrems-II judgment, the European Data Protection Board has added a specific disclaimer related to the now required case-by-case assessments:

“In accordance with the judgment of the Court of Justice of the European Union C-311/187, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, [Company Name] and its Group Companies should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.”

About TrustArc

TrustArc automates the creation of end-to-end privacy management programs for global organizations. As the leader in privacy compliance and data protection, TrustArc is the only company to deliver the depth of privacy intelligence that’s essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco, and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk and build trust. In 2019, TrustArc acquired Nymity to accelerate the development of its next-generation technology-driven privacy platform. For additional information visit www.trustarc.com.