



# Trans-Atlantic Data Privacy Framework : New perspectives for personal Data Transfer to the United States

Legal & Compliance impact  
July 2022



**EY**

Building a better  
working world



# Table of contents

## Contents

1	Context and background: The invalidation of the Privacy Shield	4
2	What will be the implications of the new Trans-Atlantic Data Transfer Framework	8
3	Pending the adoption of the new framework, what precautions to take when transferring personal data to the United States and other third countries ?	12
4	Sanctions applicable in case of Data Breach	16
5	Summary & what to expect	18





### Introduction

The GDPR (General Data Protection Regulation) is a European regulation that came into effect as from May 25<sup>th</sup>, 2018. Its purpose is to **provide a set of standardized data protection laws across all the member countries.**

This regulation makes it easier for EU citizens to understand how their data is being used, and allows them to raise complaints more easily, even if they are not in the country where it is located.

In this context, the GDPR also imposes restrictions on the transfer of personal data outside the EU, to the so-called third-party countries or international organizations. It does so by determining the legal grounds and defining the conditions for such a transfer, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

One of those legal grounds is the **"Adequacy decision"**. This refers to the situation whereby the transfer of personal data to a third country or an international organization may take place because the EU Commission has decided that this third country, a territory or one or more specified sectors within that third country or international organization ensures an adequate level of protection. When assessing this, the Commission shall, in particular, take the following elements into account :

- ▶ The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral
- ▶ The existence and effective functioning of one or more independent supervisory authorities
- ▶ The international commitments the third country or international organization concerned has entered into.



#### Adequacy decision

The situation whereby the transfer of personal data to a third country or an international organization may take place because the EU Commission has decided that this third country, a territory or one or more specified sectors within that third country or international organization ensures an adequate level of protection.

# 1

## CONTEXT AND BACKGROUND

### The invalidation of the Privacy Shield





## What was the Privacy Shield's Adequacy Decision ?

The Privacy Shield was an informal agreement between the United States and the European Union, intended to ensure compliance with European data protection standards for data transfers to the United States. The agreement was negotiated with the Obama administration and adopted by the EU Commission as an **adequacy decision** on July 12<sup>th</sup>, 2016.

The Privacy Shield included a number of assurances from the U.S. government. However, as from its inception, it was criticized by data protectionists and civil rights organizations for keeping open the possibility of mass surveillance by U.S. authorities.

In July 2020, the European Court of Justice (CJEU) overturned the agreement (the so-called Schrems-II decision), thus removing the legal basis for all data transfers based on it. Indeed, it held that the Privacy Shield and the U.S. law was incompatible with the GDPR because of the use by the American authorities of data transferred from the EU to the United States, in the context of Intelligence activities, were not limited to the strict necessary. In practice, e.g. the FBI and the CIA still had/forced access to data in a much more intrusive manner than what would be compliant with GDPR.

Nevertheless, in the same Schrems-II decision invalidating the Privacy Shield, the CJEU confirmed the validity of the European Standard Contractual Clauses (**SCCs**) for the data transfer to third countries or organizations.

## What are SCCs?

According to the GDPR, SCCs are defined as model contract clauses that have been "pre-approved" by the European Commission, and that ensure appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries.

In its decision of July 2020, the CJEU emphasized the specific additional obligations as imposed by the SCCs, not only on the exporter but also on the data importer, to assess whether the third country recipient (including subsidiaries, parent companies and third-party service providers) can meet the requirements of the SCCs in practice. If not, the data exporter will not be able to enter into a relationship or will have to suspend or even terminate the data transfer.

This results in a material impact for companies, since any data transfer under the privacy shield could principally benefit from a legal framework before (i.e. the Privacy Shield), whilst after the judgement invalidating that Privacy Shield, every data transfer to the United States needed to be subjected to an individual assessment to determine whether or not it met the criteria of the judgement.

## Consequences and impact of the Privacy Shield invalidation

Data transfers on the basis of the Privacy Shield framework became illegal after the judgement and they needed to cease without a grace period.

Regarding the use of SCCs instead of the Privacy Shield, the CJEU found that U.S. law itself does not ensure an equivalent level of protection. Whether or not your data transfer can be based on SCCs thus depends on the result of each individual data transfer assessment, considering the concrete circumstances of the transfers, and supplementary measures to implement.

The transfer of personal data from European organizations to U.S. organizations by using the SCCs is therefore very complex and requires an individual assessment (and/or measures to be taken).

It has become necessary to adopt a new agreement on data transfer between Europe and the United States. However, the difficulty is that the U.S. law has been found inadequate (from a data protection perspective), which makes it more difficult to use the SCCs, even though they were made mandatory to transfer data to the United States, as the Privacy Shield has been declared invalid.

To mitigate the above, in March 2022, The European Commission and the United States announced an agreement on a new "**Trans-Atlantic Data Privacy Framework**". In this context, this paper explores the following questions:

- ▶ What will be the impact of the new Trans-Atlantic Data Transfer Framework ?
  - ▶ What ?
  - ▶ When?
- ▶ Pending the adoption of this new framework, what precautions should already be taken when transferring personal data to the United States?





# 2

## What will be the implications of the NEW TRANS-ATLANTIC DATA TRANSFER FRAMEWORK



## What does it mean in practice ?

The European Commission and the U.S. Government adopted a new Trans-Atlantic Data Transfer Framework to be published, which will impact existing requirements.

Deadlocking on European data transfer to the United States

It will be possible for personal data to flow freely and securely between the EU and the participating U.S. companies.

Binding restrictions of the access to data by U.S. intelligence services

A new set of rules and binding protective measures will restrict the access by U.S. intelligence services. This ensures that access takes place only if it is necessary and proportionate to ensure national security, without disproportionately affecting the rights and freedoms of individuals. Procedures are being established to ensure effective monitoring of the new standards.

Creation of a Data Protection Court

A new two-tier redress system will ensure that complaints from EU citizens about access to data by U.S. intelligence services are investigated and dealt with. A new and independent "Data Protection Review Court" is being set up for judicial review.

Maintain of self-certification for U.S. companies

There are strict obligations for U.S. companies that process data transferred from the EU. This includes, in particular, the obligation to confirm compliance with the agreement to the U.S. Department of Commerce by means of **self-certification**.

In Compliance with the European Framework, the U.S. White House's declaration confirms that the new Framework will ensure:

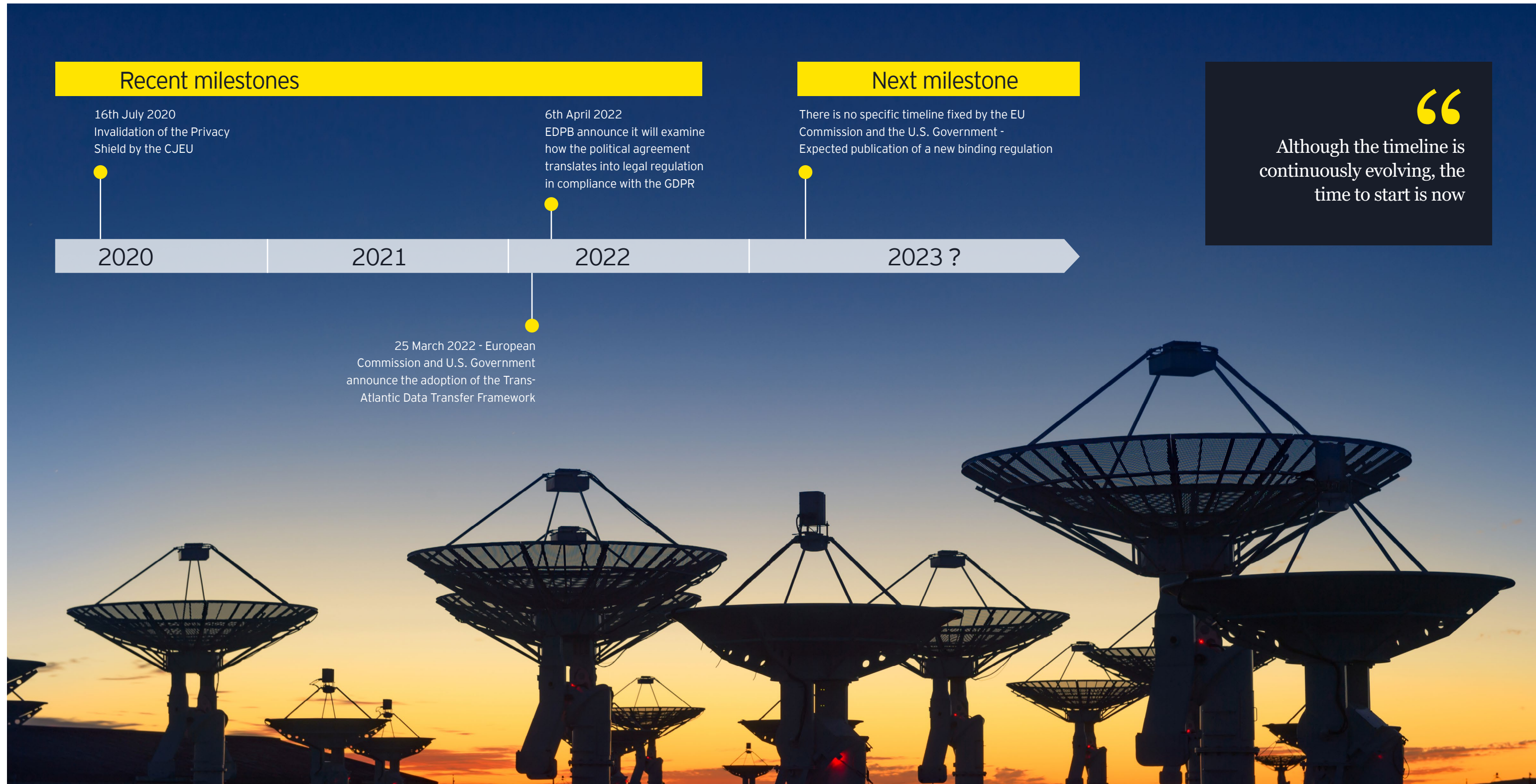
- ▶ Signals intelligence collection may be undertaken only where necessary to advance legitimate national security objectives, and must not disproportionately impact the protection of individual privacy and civil liberties.
- ▶ EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent Data Protection Review Court that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed. The EDPB emphasizes that any "new authority" set up under a claim of delivering redress will need "access to relevant information, including personal data" in order to be able to live up to that mission and will also need to be able to adopt decisions that are binding for the intelligence services.
- ▶ U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

The exact and concrete content of this legal framework has not yet been published. Only initiatives and intentions (of the direction it will take) are available at this point in time. Nevertheless, it is already clear that there will be a material impact for companies (including financial institutions) and actions will need to be taken, such as :

- ▶ Mapping the data currently shared with U.S. companies, and the contractual clauses currently in place
- ▶ Implementing new internal measures to terminate the potential suspension of the data transfer with U.S. companies,
- ▶ Reviewing the temporary corrective measures adopted to compensate for the lack of a regulatory framework legitimizing the abovementioned transfer, notwithstanding the invalidation of the Privacy Shield.

Once the final framework has been published, an in-dept analysis will be provided to determine what exact measures and actions need to be taken.

## When ?



“  
Although the timeline is continuously evolving, the time to start is now

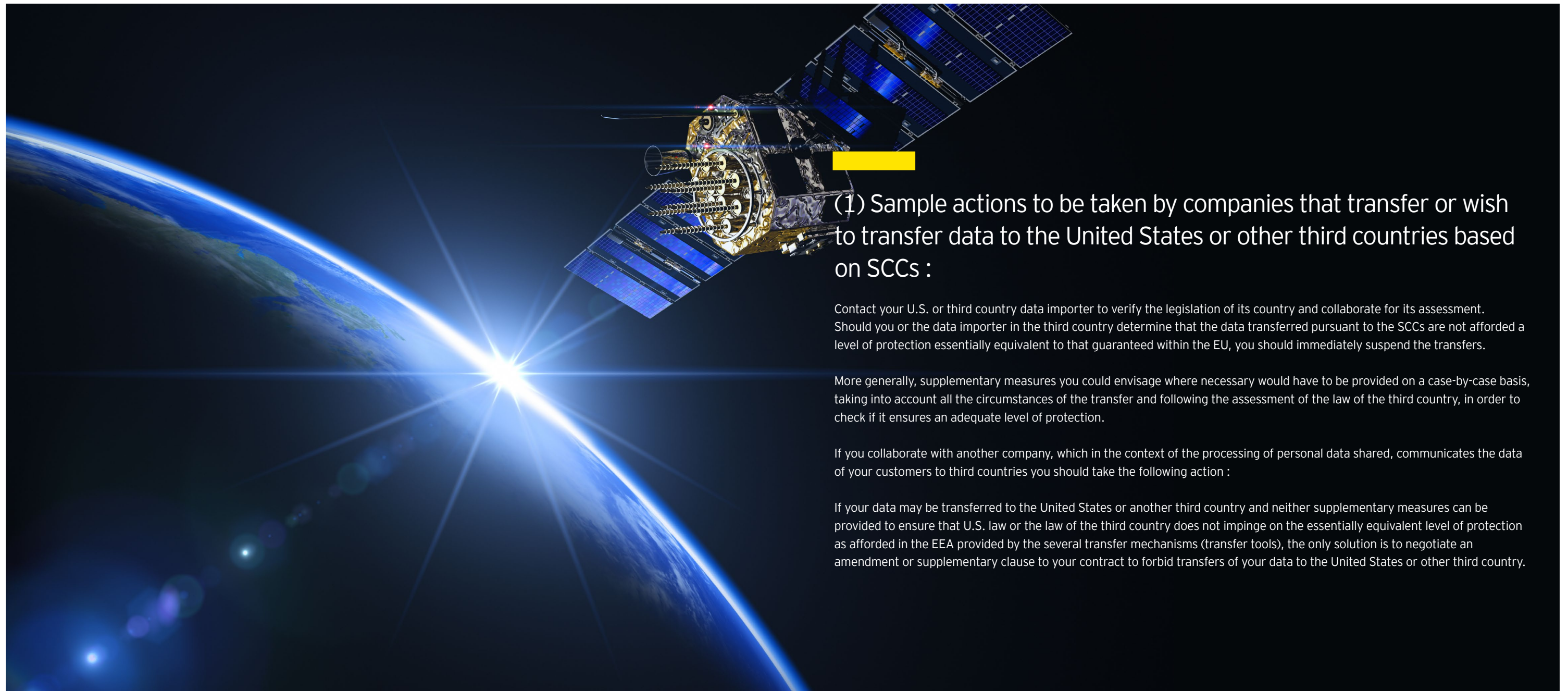


# 3 Pending the adoption of the new framework WHAT PRECAUTIONS TO TAKE WHEN TRANSFERRING PERSONAL DATA to the United States and other third countries ?

## Precautions companies should take when transferring personal data to the United States and others third Countries

Pending the publication of the Trans-Atlantic Data Transfer framework, companies transferring personal data to the United States at this point in time should take the following in mind to be compliant:

- The sample actions to be taken by companies that transfer or wish to transfer data to the United States and other third countries based on SCCs (1)
- The European Data Protection Board's ("EDPB") guidelines for data transfers to the United States and other third countries (2)



### (1) Sample actions to be taken by companies that transfer or wish to transfer data to the United States or other third countries based on SCCs :

Contact your U.S. or third country data importer to verify the legislation of its country and collaborate for its assessment. Should you or the data importer in the third country determine that the data transferred pursuant to the SCCs are not afforded a level of protection essentially equivalent to that guaranteed within the EU, you should immediately suspend the transfers.

More generally, supplementary measures you could envisage where necessary would have to be provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection.

If you collaborate with another company, which in the context of the processing of personal data shared, communicates the data of your customers to third countries you should take the following action :

If your data may be transferred to the United States or another third country and neither supplementary measures can be provided to ensure that U.S. law or the law of the third country does not impinge on the essentially equivalent level of protection as afforded in the EEA provided by the several transfer mechanisms (transfer tools), the only solution is to negotiate an amendment or supplementary clause to your contract to forbid transfers of your data to the United States or other third country.

(2) The EDPD recommends a 5-step due diligence process to ensure the legality of data transfer to any third country (not only regarding the United States):



1. Know your transfer

In case of the existence of an adequacy decision:

- ▶ You must map all transfers of personal data to third countries.
- ▶ You must be aware of where the personal data goes. This is necessary to assess whether or not it is afforded an essentially equivalent level of protection wherever it is processed.
- ▶ You must verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

2. Verify your transfer tools

In case of the existence of an adequacy decision :

- ▶ As long as the decision is still in force, you will not need to take any further steps, other than monitoring that the adequacy decision remains valid.

In the absence of an adequacy decision (such as with the United States at this point in time) :

- ▶ You need to rely on one of the transfer tools listed under Articles 46 GDPR, which are binding corporate rules, SCCs, approved code of conduct, approved certification mechanisms.
- ▶ Only in some cases are you able to rely on one of the derogations provided for in Article 49 GDPR if you meet the conditions, which are explicit consent, certain forms of contract execution, public or vital interest, defence of legal claims,...
- ▶ Derogations cannot become “the rule” in practice, but need to be restricted to specific situations.

3. Assess

Make an assessment to verify if there is anything in the law and/or practices in force 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.

You must also examine the practices of the third country’s public authorities, which will allow you to verify if the safeguards contained in the transfer tool can ensure, in practice, the effective protection of the personal data transferred. It will be especially relevant for your assessment where:

- ▶ Legislation in the third country formally meeting EU standards is manifestly not applied/complied with in practice
- ▶ There are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking
- ▶ Your transferred data and/or importer falls or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool’s contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality).

In the absence of an adequacy decision, you will have to suspend the transfer or implement adequate supplementary measures to guarantee the level of protection is equal to what is required in the GDPR, if you wish to proceed with it. In the third situation, in light of uncertainties surrounding the potential application of problematic legislation to your transfer, you may decide to:

- ▶ Suspend the transfer
- ▶ Implement supplementary measures to proceed with it
- ▶ Or proceed with the transfer without implementing supplementary measures if you consider and are able to demonstrate and document that you have no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice so as to cover your transferred data and importer.

You should conduct this assessment with due diligence and document it thoroughly as the competent supervisory and/or judicial authorities may request it and hold you accountable for any decision you take on that basis.

**This is the case now for data transferred to the United States, with the invalidation of the Privacy Shield.**

4. Identify and adopt supplementary measures

It is relevant to 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 and/or practices impinge on the effectiveness of the transfer tool you are relying on or you intend to rely on in the context of your transfer.

Example of measures to be implemented :

- ▶ Performing regular audits of strong disciplinary measures, that should be in place to monitor and enforce compliance with the data minimization measures in the transfer context and the performance of assessment of the personal data before the transfer takes place.
- ▶ By doing so, performing an identification of data sets that are not necessary for the purposes of the transfer and, therefore, won’t be shared with the data importer.

**You may need to build up a plan and to consult your competent supervisory authorities on this.**

5. Re-evaluate

One should re-evaluate, at appropriate intervals, the level of protection afforded to the personal data you transfer to third countries and monitor if there have been or will be any developments that may affect it. The principle of accountability requires continuous vigilance of the level of protection of personal data.

Supervisory authorities will continue to exercise their mandate to monitor the application of the GDPR and enforce it.

Supervisory authorities will pay due consideration to the actions exporters take to ensure that the data they transfer is afforded an essentially equivalent level of protection.

As the CJEU recalls in its Schrems-II decision, supervisory authorities will suspend or prohibit data transfers in those cases where they find that an essentially equivalent level of protection cannot be ensured, following an investigation or a complaint. Supervisory authorities will continue to develop guidance for exporters and coordinate their actions in the EDPB to ensure consistency in the application of EU data protection law.



# 4

## SANCTIONS

applicable in case of Data Breach

### What are the foreseen sanctions ?

Under the GDPR, the national Data Protection Authorities (DPA's) has the right to impose large administrative fines on companies that transfer data abroad illegally. Data subjects also have the right to request the suspension of the transfer, and to engage the civil liability of the company in order to obtain compensation for the material and/or moral damage suffered.

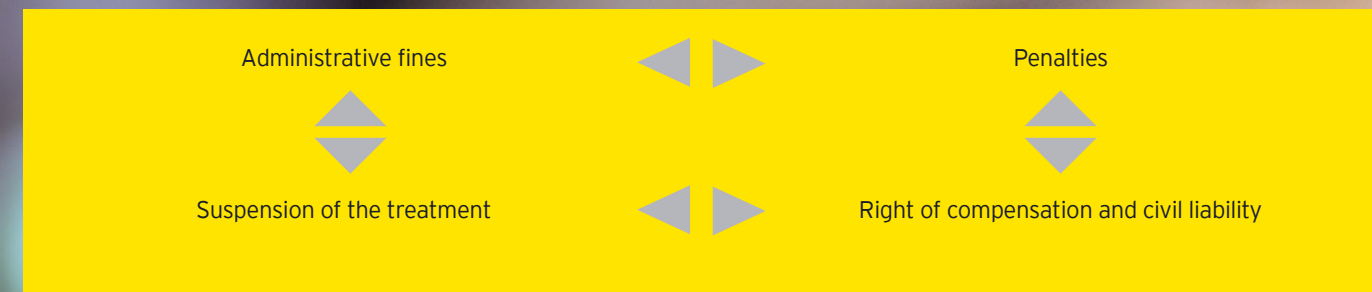
Finally, the Public Ministry of the State can prosecute the company.

**Administrative fines by the DPA**

In case of illegal transfer, the Data Protection Authority can require infringers to comply and, if necessary, impose administrative fines of up to 20 million euros or 4% of the company's total revenue. Other infringements of the GDPR provisions can be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

**Penalties**

In Belgium, illegal transfer of personal data to a third country is a criminal offence that can lead to prosecution and fines of several tens of thousands of euros to even millions of euros.





# 4 SUMMARY & what to expect



## Summary & what to expect

Data transfers to U.S. companies are permitted if they comply with the GDPR. Adequacy was once guaranteed by the "Privacy Shield", but the CJEU declared invalid this Privacy Shield which allowed data to be transferred between the European Union and U.S. companies, while declared valid the use of the SCCs.


The consequences of the annulation of the Privacy Shield for companies are:

- Data transfers on the basis of the Privacy Shield framework became illegal and must cease. There is no grace period during which an EU company can keep on transferring data to the United States without assessing a legal basis for the transfer.
- If using SCCs instead of the Privacy Shield, the financial institution shall remind that the CJEU found that U.S. law does not ensure an essentially equivalent level of protection. Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place.

To mitigate this difficult situation, The European Commission and the United States announced an agreement on a new "**Trans-Atlantic Data Privacy Framework**" that should address the impossibility of transferring data to the United States.

The content of this legal framework has not yet been published, but we can certainly foresee that its impact will be for companies (including financial institutions) to take action such as to implement new internal measures to terminate the potential suspension of the data transfer to U.S. companies, as well as to review the temporary corrective measures adopted to compensate for the lack of a regulatory framework legitimizing the abovementioned transfer, notwithstanding the invalidation of the Privacy Shield. An evaluation of data-sharing practices involving data transfers to the United States may be necessary, particularly at the level of financial institutions.





## Your EY contact



**Filip Bogaert**  
Partner  
Legal  
filip.bogaert@be.ey.com  
+32 477 631 462

EY | Assurance | Tax | Strategy and Transactions | Consulting  
About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). For more information about our organization, please visit [ey.com/be](https://ey.com/be)

EY is a leader in serving the financial services industry

We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions. The better the question. The better the answer. The better the world works.

© 2022 EYGM Limited - All Rights Reserved - ED None  
This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.