Complior

GUIDE TO UNDERSTANDING GDPR AND DATA TRANSFERS FOR CLOUD HOSTED DATA

MAY 2021

INTRO

The European Commission takes personal data of its citizens very seriously and penalizes organizations that are not up to date and following protocols, no excuses granted. Understanding GDPR, implications of the annulment of the Privacy Shield and specifics around transfer mechanisms is all up to each individual business. For many small and medium businesses IT services, like hosting servers and ERP platforms, are third party SaaS cloud solutions.

Where exactly is data stored when using a cloud hosting provider, and what are the legal requirements of transferring this data within and outside the EEA? From the US' Cloud Act, to BCR and the background on why the Privacy Shield is no more, Complior has all the information you need in this guide to evaluate and take measures to protect your business.

Working behind the scenes with an ear on government regulations and spearheading innovative solutions when changes come down the pipeline for our partners long before you even read about them is the name of our game. Many of the questions you may have will be found within this guide, for anything additional please don't hesitate to contact our team of experts at Complior.

IN THIS GUIDE:

WITHOUT THE PRIVACY SHIELD, ARE YOUR DATA TRANSFERS LEGAL?

The General Data Protection Regulation (GDPR) demands that the protection granted to personal data in the European Economic Area (EEA); the EU, Iceland, Liechtenstein and Norway, must travel with the data wherever it goes. Any and all transfers of personal data outside of the EEA must be able to provide similar safeguards for personal data as in the EEA. Privacy Shield was a legal framework and a special agreement between the US and EU that was the most common legal basis for organizations to transfer personal data to the US legally under the GDPR. Organizations in the US needed to self-certify to Privacy Shield through the U.S. Department of Commerce's International Trade Administration.

On July 26, 2020 the Schrems II case in the European court of justice marked the end of Privacy Shield.

What is the Schrems II case?

The first Schrems case, named after the plaintiff Max Schrems, a lawyer and privacy activist, resulted in the annulment of privacy principles between the EU-US named 'Safe Harbour'. Safe Harbour was the predecessor to Privacy Shield. Schrems used that he was a Facebook user as a vector to attack Safe Harbour, since his personal data was transferred to the US where Facebook stores its data. His timing aligned with the Snowden controversy in the US and Schrems won the case resulting in the annulling of Safe Harbour. After the disappearance of Safe Harbour, the EU made another agreement with the US similar to that of Safe Harbour – Privacy Shield. Now the Schrems II judgement has annulled Privacy Shield as well.

With the Privacy Shield annulled, organizations must find another way to make the transfer legal under the GDPR.

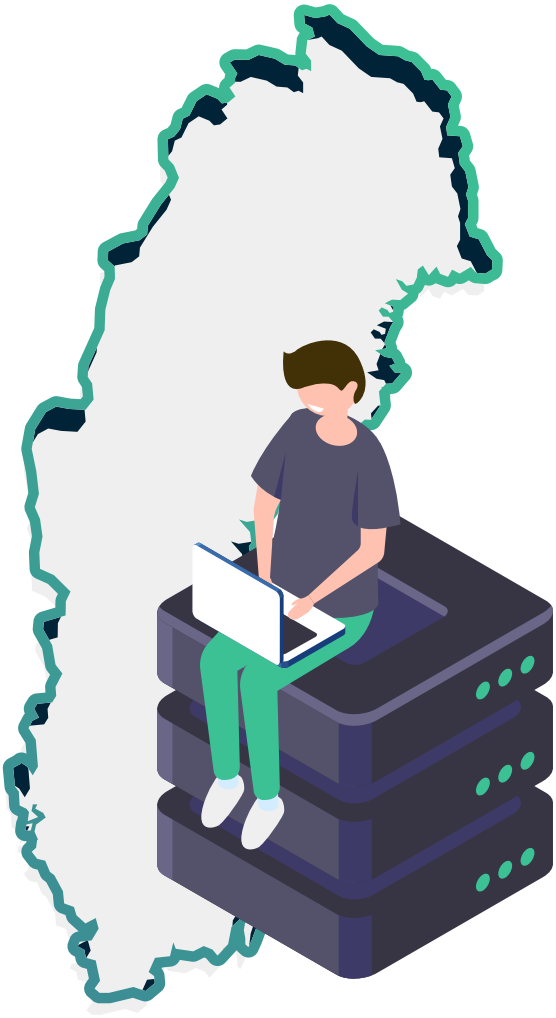
Any country outside of the EEA is defined as a third country in the GDPR. Chapter 5 in the GDPR starts by saying that transfer of personal data, meaning that information is either transferred or accessible to parties outside of the EAA, is only legal if it is listed as having adequate levels of protection. With the Privacy Shield gone the US no longer meets privacy requirements, therefore a transfer mechanism such as Standard Data Protection Clauses or Binding Corporate Rules (BCR) is required. These transfer mechanics may need supplementary safeguards if the law of the importing third country impinges on the effectiveness of the appropriate transfer mechanics. Even so, you may still face legal challenges resulting from the CLOUD Act with the absence of EU-US international agreements such as MLATs. (*For a deeper understanding of transfer mechanics, clauses and the CLOUD Act see the next chapter.)*

Organizations should evaluate the risks of using a US-based cloud service and assess if the risks are acceptable. If you are an organization that transfers personal data to the US or any other third country, to ensure your transfers stay legal we suggest following the following **five steps as outlined by the EDPB Recommendations 01/2020:**

1. **Know your transfers.** Map out the third country transfers in your organization.
2. **Verify the transfer tool your transfer relies on.** Identifying the third country is on the list of countries with adequate levels of protection or what transfer mechanic is used.
3. **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.
4. **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. Depending on the transfer mechanic in article 46 you may need to consult your supervisory authority.
5. **Re-evaluate** at appropriate intervals the level of protection afforded to the data you transfer to third countries and monitor if there have been or there will be any developments that may affect it.

Strictly speaking, EU organizations risk data violation under the GDPR if using US-based cloud services because of the CLOUD Act and other uncertainties regarding how abstract the current supplementary measures to the transfer mechanics are. It may be beneficial to organizations to choose a local EEA based cloud or hosting provider that follows GDPR instead. This is especially true for organizations that handle very sensitive personal data, such as authorities, health care providers, banks, and insurance companies. Sensitive data will require more stringent safeguards and cause higher administrative sanctions if there is a data violation under the GDPR.

Switching hosting providers to a local EEA company is easier than many may think. Our team of experts at Complior place security first to ensure all data is safely transferred with minimal downtime and ready to go backup protocols in place. With security requirements of utmost importance to our clients we are always monitoring, troubleshooting and implementing new regulations as they are announced. GDPR can be intimidating and a resource depletion for small to medium sized businesses. Complior offers managed hosting solutions for EEA organizations as well as GDPR services to help you fulfill the requirements, protect your data and focus on your core clients and services.



UNDERSTANDING TRANSFER MECHANISMS IN GDPR

Let's start with the basics on how you can make lawful transfer of personal data from the EEA to the rest of the world. It's worth noting that the transfer of personal data means both that information is accessible by or transferred to parties outside of the EAA. Any country outside of the EEA is defined as a third country in the GDPR. Chapter 5 in the GDPR starts by saying that transfers to a third country or international organization is only legal if one of the conditions or **transfer mechanisms** in that chapter is met.

The first **transfer mechanism** is that the third country, or the international organization in question, ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. The European Commission has a list of third countries it deems adequate on their website. Their assessment of adequacy is based on that country's rule of law concerning human rights and freedoms. This is the current list as of Feb 2021: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The USA was removed from this list when Edward Snowden showcased privacy issues concerning the US' approach to internet surveillance.

Not all countries can assure a similar data protection to the GDPR like those on the list, hence there are a few other transfer mechanisms in place. Another transfer mechanic is ensuring there is an appropriate safeguard in place. The two most common safeguards are the Standard Data Protection Clauses and Binding Corporate Rules.

Standard Data Protection Clauses

The European Commission has issued two sets of standard contractual clauses for transmitting personal data from one controller in the EU to another controller in a third country, and one set for controller to processor transfers. The standard contractual clauses are basically a contract template of clauses that you can use on their own or incorporate in a wider contract if you do not modify the clauses or add contradictory clauses. The clauses regulate things commonly seen in Data Protection Agreements, for example, reporting commitments in case of a personal data breach.

Binding Corporate Rules (BCR)

Written policies or rules that international organizations create for themselves to be able to regulate their transfer of personal data outside of the EU within their group of undertakings or enterprises. The main supervisory authority for the international organization must review and authorize the BCR before it can be used as a transfer mechanism under GDPR. For BCR rules to be valid, the international organization must be able to comply with their BCR in practice.

The European Data Protection Board (EDBP) recently released new recommendations following the Schrems II judgement, saying that transfer mechanics do not operate in a vacuum and may need to be supplemented with other measures if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards or transfer mechanics. They do not say anything on what those measures are.

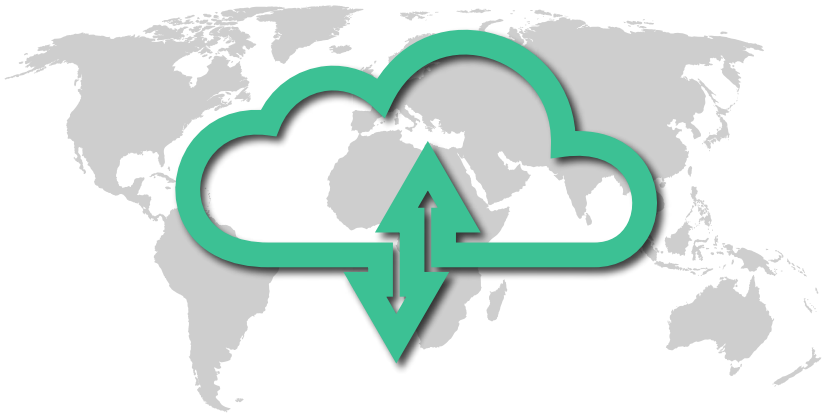
An Example

Erlanders Group is among the first international organizations in Sweden to have their BCR accepted by the Swedish supervisory authority and may freely transfer personal data within their group. However, they also say that the Erlanders Group must adhere to their BCR in practice and verify that the law of the importing third country makes it possible to provide a level of protection of personal data that is broadly equivalent to that provided within the EU. They also mention that a risk assessment should be used for determining the safeguards in the third country regarding the data subject's rights and freedoms.

WHAT IS THE CLOUD ACT?

The Cloud Act is a United States federal law enacted in 2018, that asserts U.S. data and communication companies must provide stored data for a customer or subscriber on any server they own when requested by warrant from a US law enforcement agency. However, the act contains mechanisms for the companies or the courts to challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in.

The European Data Protection Supervisor (EDPS) and the EDBP view the Cloud Act as a law in possible conflict with the GDPR and has made an official review of the act. They point out that Article 48 of the GDPR requires that any order from a non-EU authority requiring the transfer of personal data outside the EEA must be recognized by an international agreement (i.e. MLAT) to be valid. A quote from the official report, "We are of the view that currently, unless a US Cloud Act warrant is recognised or made enforceable on the basis of an international agreement, the lawfulness of such transfers of personal data cannot be ascertained..." Therefore, they have proposed that it's urgent to create new MLATs between the EU and US so the Cloud Act can be incorporated in the EU's legal framework, since today it is not.



The problem for organizations is that many fall under US jurisdiction. Businesses that utilize cloud storage solutions owned by a US company or even EU organizations that just have US customers or subscribers technically fall under US jurisdiction.

An EU-based company fulfilling a warrant that has been issued by a US court requiring the transfer of personal data is today in breach of article 44 and 48 of the GDPR if there is no international agreement in place. However, if the organization does not fulfill the warrant, they will be breaching US law instead.

Naturally, organizations do not want to be in this position where they need to choose which law they should follow. As of now there is no crystal clear right way until further legislation is enacted. That's why partnering with a team of experts like ours at Complior ensures you can navigate these types of situations and are following the latest legal requirements as they become valid. With so much of the world quickly moving online due to current circumstances, regulations and laws are changing and adapting quicker than ever. It is easy to get penalized for something your organization truly missed, yet is accountable to implement. Choosing local and secure cloud hosting partners like Complior in Sweden minimizes issues that could arise from things like the Cloud Act in the US.


Complior