Securing Access to Data in a Post Schrems II Era
## Contents

### 3 Introduction

### 3 What is the Schrems II ruling?
- What gaps in GDPR does Schrems II address?
- How does Schrems II impact your privacy program if no action is taken?

### 4 GDPR – A Primer
- What is GDPR?
- Why was GDPR created?
- Who does GDPR apply to?
- Who within a company is responsible for compliance?
- What types of data does GDPR protect?
- What are the consequences of non-compliance?

### 6 Recommendations for Closing Gaps in GDPR
- EDPB Recommendations on Supplementary Measures
- EU Essential Guarantees for Non-EU Countries

### 7 Access Security for Schrems II Compliance

### 8 Benefits of a cloud agnostic access security solution
- Maintain regulatory compliance now and tomorrow.
- Control your own access security.
- Limit the inheritance of threats and breaches.
- Avoid the dangers of vendor lock-in.

### 9 The benefits of Thales SafeNet Trusted Access

### 9 Conclusion

### 9 About Thales
Introduction

The Schrems II decision will have a great impact on international commerce among companies doing business with the European Union (EU). The consequence of not paying attention to Schrems II could literally mean a partial or complete shut-down of data transfers between EU and non-EU countries, which could impact the bottom line of any global company. However, the level of the impact depends on the location of the company, the industry vertical it is part of, and the strategic privacy planning that company has done for sustaining compliance with General Data Protection Regulation (GDPR).

GDPR requires businesses to protect the personal data and privacy of European Union (EU) citizens, for any transactions that occur within EU member states. GDPR also regulates exportation of personal data outside the EU to some extent. But, there are gaps in its enforcement of transactions flowing outside the EU, which are addressed by the Schrems II ruling.

The purpose of this whitepaper is to demonstrate how a strong and effective access security solution, like Thales SafeNet Trusted Access, can help multinational companies adhere to the recommendations of the European Data Protection Board to ensure lawful data transfers in accordance with the Schrems II ruling.

Schrems II – Identifies the Gaps in GDPR

What is the Schrems II ruling?

The Schrems II ruling was issued by the Court of Justice of the European Union (CJEU) in July 2020. In this case - Data Protection Commissioner Vs Facebook Ireland and Maximillian Schrems, the Irish Data Protection Commissioner issued an order instructing Facebook to stop transferring the data of EU users to the United States. The European court found that EU-US Privacy Shield Framework, which permitted companies to freely transfer users’ personal data, illegally infringed EU residents data protection and privacy rights, and argued that the US surveillance law (FISA) does not provide adequate protections or remedies for non-US persons in the EU.

What gaps in GDPR does Schrems II address?

The General Data Protection Regulation (GDPR) laid down the requirements on securing personal data within the European Union (EU) or European Economic Area (EEA). However, it does not adequately address securing personal data of EU citizens when it is processed outside the EU by other countries. That’s exactly what the Schrems II ruling identified as the gaping hole in GDPR.

How does Schrems II impact your privacy program if no action is taken?

The Schrems II decision invalidates the Privacy Shield Framework, since it did not adequately enforce EU’s GDPR regulations to protect personal data as it moved between EU and the US. With the nullification of Privacy Shield, and before that, Safe Harbor, companies are no longer protected from liability over those data transfers and they are looking for data protection solutions that can adequately protect global commerce. With regulators on both sides of the Atlantic heading back to the regulatory drawing board, thousands of multinational organizations are now in legal limbo. This decision directly impacts transatlantic digital commerce that account for more than half of Europe’s data flows.
GDPR – A Primer

Let’s step back and understand the purpose of the General Data Protection Regulation (GDPR), before we think about the comprehensive data protection solutions needed to addresses GDPR mandates as well as resolve the challenges of Schrems II.

What is GDPR?
The General Data Protection Regulation (GDPR) was adopted on 14 April 2016, and became enforceable beginning 25 May 2018. As GDPR is a regulation (a law that can be enforced) and not a directive (not enforceable), it is directly binding for all companies doing business with the EU. GDPR supersedes the Data Protection Directive 95/46/EC, which contained requirements related to processing of personal data of individuals (formally called data subjects in GDPR).

Why was GDPR created?
GDPR was created in Europe to address the public concerns of EU citizens over privacy. These concerns grew from high profile security breaches happening over many years. The primary goal of GDPR is to give individuals control over their personal data, so that they are not misused or exposed by businesses who are controlling and processing their data.

Who does GDPR apply to?
Any company that stores or processes personal information about EU citizens in the European Economic Area (EEA) must comply with GDPR, even if the company is not located in the EU. Here are the specific criteria that is applicable to companies who need to comply.

- Company has presence in any EU country
- Company has no presence in the EU, but they process personal data of EU residents
- Company size is bigger than 250 employees
- Company size is smaller than 250 employees, but its data-processing impacts the rights and freedoms of data subjects, or includes certain types of personal data.

Who within a company is responsible for compliance?
GDPR defines the following roles that are responsible for ensuring compliance: Data Controller, Data Processor, and the Data Protection Officer.

- **Data Controller:** will be the one who dictates how and why data is going to be used by the organization. They control what data is shared with third-parties, and ensure that those third parties comply with data privacy controls.
- **Data Processor:** simply processes the data that the Data Controller gives them. A Data Processor could be a third-party company within or outside the EU. The third-party does not own the data that they process, nor do they control it.
- **Data Protection Officer (DPO):** GDPR requires the controller and processor to designate a DPO to oversee data security strategy and GDPR compliance. Companies are required to designate a DPO, if they process and store large amounts of EU citizen data.
What types of data does GDPR protect?

According to GDPR: “personal data” means any information relating to an identified or identifiable natural person (“data subject”) It includes any of the following data types.

- Personal Identifiable Information (PII) such as name, address, ID numbers (driver’s license, Tax ID)
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Racial and ethnic data
- Political opinions
- Sexual orientation

What are the consequences of non-compliance?

The consequences on non-compliance cross geographical boundaries.

**Fines**

The regulation imposes a strict data protection compliance regime with severe penalties of “up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”

**Breach notification**

In addition, in the case of a breach of personal data, the organization breached will be required to notify the subjects of the breach “without undue delay.” A timeline of 72 hours has been highlighted in the official documentation.
Recommendations for Closing Gaps in GDPR

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout EU, and promotes cooperation between data protection authorities in each EU country. EDPB recently adopted recommendations on supplementary measures along with a second document on EU essential guarantees, to address the gaps identified by the Schrems II ruling.

EDPB Recommendations on Supplementary Measures

The European Data Protection Board recommends the following six-step plan to continually assess and protect global data flows in-line with the EU data privacy regulations.

**Step 1: Know your data transfers**
The first step is to ensure that you have a record of all data transfers with other countries outside the EU logging the series of data processors and sub-processors. You must identify that the data you transfer is adequate, relevant and limited to what is necessary to be processed in the third country.

**Step 2: Identify the transfer tools you are relying on**
The second step is to identify the data transfer tools you are relying on among those listed in Chapter V of GDPR, take decisions relating to some or all of the third countries to which you are transferring data, and ensure that they offer adequate level of protection of personal data.

**Step 3: Assess whether the transfer tool is sufficient to meet GDPR requirements**
The transfer tool must ensure that the level of protection guaranteed by GDPR (article 46) within the EU countries is as good in the third country outside the EU. Your assessment should take into consideration all the actors participating in the data transfer (e.g. data controllers, processors, and sub-processors).

**Step 4: Adopt supplementary measures**
If the assessment in step 3 has revealed that the transfer tool is not effective, then you will need to consider supplementary measures, which when added to the safeguards could ensure the same level of safeguards guaranteed within the EU are enforced in external data transfers.

**Step 5: Procedural steps if you have identified supplementary measures**
You may have to take these supplementary measures, if the primary measures used by the data transfer tools are not sufficient to protect the data.

**Step 6: Re-evaluate at appropriate intervals**
You must monitor on an ongoing basis, and where appropriate in collaboration with the data importers in the third countries to which you have transferred data, put in sufficient mechanisms to promptly suspend data transfers, if the data importer breached the contract.

EU Essential Guarantees for Non-EU Countries

The aim of the European Essential Guarantees is to provide elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, can be performed by national security agencies or law enforcement authorities, in a responsible manner without jeopardizing the privacy of the EU citizen.
Here are the four European Essential Guarantees that specify further how to assess the level of interference with the fundamental rights to privacy, and to protect data in the context of surveillance.

**Guarantee A**
Processing should be based on clear, precise and accessible rules on interception of data transfers. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to any such measures.

**Guarantee B**
Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated. The necessity of the interference must be proportional to the seriousness of the offense, only if the concerned non-EU state is confronted with a serious threat to national security.

**Guarantee C**
Independent oversight mechanism should be present in relation to surveillance. The European court has expressed its preference for a judge or another body to be responsible, as long as it is sufficiently independent from the executive.

**Guarantee D**
Effective remedies need to be available to the individual through legal channels once the surveillance is over.

### Access Security for Schrems II Compliance

The EDPB recommendations allow organizations to build a trusted privacy framework for transatlantic data flows which is based on the following overarching principles:

- **Discover your data wherever it is and classify it.** That way you know what data you have so you can apply the appropriate security measures as outlined by GDPR.
- **Protect sensitive data in motion and wherever it is stored using robust encryption.** Encrypting network traffic and data stored in the cloud and data centers ensures that no one can read the data.
- **Control access to data** by managing access credentials in the country of the origin of the data. That way, you control access to the data, reducing the chance that a cloud provider or government can access the data.

The problem with lawful data process and storage stems from the fact that the major cloud service providers are not based in the European Economic Area (EEA) region. This raises certain concerns regarding the access of EU personal data. The European Data Protection Board (EDPB) has identified two Unlawful Use Cases:

- **Unlawful Use Case 6** Transfer to cloud services providers or other processors which require access to data in the clear.
- **Unlawful Use Case 7** Remote access to data for business purposes.

The existence of Unlawful Use Cases 6 and 7 means that common cloud vendor practices leave corporate officers and boards of directors open to liability risks originating from potential unlawful data access.

The European Union Court of Justice (CJEU) has noted that “the obligation imposed on providers of electronic communications services (…) to retain traffic data for the purpose of making it available, if necessary, to the competent national authorities, raises issues relating to compatibility with Articles 7 and 8 of the Charter of Fundamental Rights of the EU.”

Furthermore, CJEU iterated that “the persons whose personal data is affected [should] have sufficient guarantees that data will be effectively protected against the risk of abuse”, in particular where personal data is subjected to automatic processing and “where there is a significant risk of unlawful access to that data.”
Selecting an access security solution to ensure compliance with the EDPB recommendations for controlling access to personal data is a critical step towards compliance with GDPR and the Schrems II ruling. Cloud service providers have lately launched native access security solutions. However, these solutions introduce several challenges for data protection and access controls, such as:

- No segregation between access controls and cloud data
- Threat inheritance
- Reduced interoperability across multiple cloud platforms
- Complexity and platform ecosystem lock-in

To meet the new data sovereignty requirements, cloud service providers have modified their Standard Contractual Clauses (SCC) to add guarantees that their services occur entirely within the EU. However, these clauses are not enough to protect against unwanted access to personal data of European citizens. The EDPB has clarified that even enabling a non-EU entity remote access for administration purposes is considered a data transfer. To satisfy the EDPB requirements for lawful transfer of EU pseudonymized data, organizations can mitigate the risks of unwanted data access by deploying their own vendor-neutral access management and authentication solution.

A cloud neutral access security solution empowers businesses to adopt policies and controls that provide the required flexibility to operate under various jurisdictions and gives organizations control over who can access data and services across these jurisdictions. Segregating duties from the cloud service provider and opting for access security solutions that meet diverse business use cases and compliance requirements is the best practice for mitigating unwanted access to personal data.

Being in control of your data protection and managing your access security policies independently of your cloud service provider, enables you to maintain compliance with GDPR and adhere to the EDPB recommendations for adopting the Schrems II ruling.

Benefits of a cloud agnostic access security solution

Segregation of security duties and adoption of an agnostic access security solution presents tangible benefits for all organizations.

Maintain regulatory compliance now and tomorrow.

The patchwork of privacy and data protection requirements requires businesses to adopt solutions to provide the required flexibility to operate under various jurisdictions while maintaining control over who can access data and services. Segregating duties and opting for authentication solutions that meet the specific operating and compliance requirements of your organization is the best practice for mitigating unlawful access to personal data.

Control your own access security.

Deploying your own, neutral solution allows you to maintain centralized, flexible control of your access security and data. Reducing reliance on - and placing less trust in your cloud service provider - results in a reduced threat surface and lowers the potential of lateral damage that could occur because of attacks on the provider.

Limit the inheritance of threats and breaches.

During the Congressional hearings for the SolarWinds attack, many participants elaborated that the use of different authentication methodologies or technologies, independent from the cloud service provider, can eliminate a considerable threat vector and introduce greater obstacles for adversaries. Considering that adversaries seek to exploit vulnerabilities to let them into networks, move laterally undetected, and exfiltrate data, increasing the level of difficulty in doing so acts as a deterrent. Cloud service providers provide great infrastructure, services, resources and apps but wrapping a neutral access security around these is considered to be best security practice.

Avoid the dangers of vendor lock-in.

Opting for a native security solution entails the danger of vendor and platform lock in. Vendor lock in presents risks from a commercial, regulatory and threat perspective, which may increase the overall risk environment. As businesses are looking to reduce their exposure to business risks and increase resilience, segregation of duties is the best practice for strengthening their security and privacy posture.
The benefits of Thales SafeNet Trusted Access

Thales is a world leader in providing vendor agnostic security solutions to help you protect your assets and data wherever they are – on-premises or in the cloud. Thales SafeNet Trusted Access lets you keep control of your access security and averts the risks of vendor lock-in.

SafeNet Trusted Access is the answer to the pain points of security and privacy stakeholders:

- IT managers can maintain flexibility by using any user directory, while strengthening business continuity by ensuring interoperability throughout multi-cloud deployments.
- The CISO can reduce attack surface and strengthen corporate security posture by separating access security from apps and data and limiting the scope of lateral attacks inside the corporate network. At the same time, they can future-proof for emerging regulations on data privacy and data sovereignty and reduce the risk of third parties accessing sensitive corporate data.
- The CFO gains flexibility and a strong negotiating position when it comes to renewals and licenses by adopting a multi-vendor strategy.

Conclusion

While GDPR is arguably the most stringent data privacy mandate ever imposed on companies within the EU, the Schrems II ruling makes it even more difficult to ensure the privacy of global data transfers beyond EU boundaries. With the nullification of Privacy Shield and Safe Harbor, companies are no longer protected from liability over those data transfers, and they are looking for access security solutions that can adequately protect their data from unlawful access. Since the fines of non-compliance could reach tens of millions of Euros, it is incumbent upon companies to implement identity protection solutions that allow for data privacy and secure access within the Schrems II guidelines.

Thales offers SafeNet Trusted Access, an industry leading access management solution that enables organizations to protect data transfers across EU and non-EU countries, helping satisfy GDPR mandates and EDPB recommendations for Schrems II.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.