

Securing GDPR-compliant Data Post Schrems II



Contents

3 Introduction

3 What is the Schrems II ruling?

3 What gaps in GDPR does Schrems II address?

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

4 GDPR – A Primer

4 What is GDPR?

4 Why was GDPR created?

4 Who does GDPR apply to?

4 Who within a company is responsible for compliance?

5 What types of data does GDPR protect?

5 What are the consequences of non-compliance?

6 Recommendations for Closing Gaps in GDPR

6 EDPB Recommendations on Supplementary Measures

6 EU Essential Guarantees for Non-EU Countries

7 Data Protection Strategies for GDPR

7 What are BYOE, BYOK and HYOK data protection strategies?

8 Why BYOE is the right strategy to address Schrems II

9 How Thales Can Help

9 Introduction to Discover, Protect, Control

10 Bring Your Own Encryption (BYOE) Offered by Thales

11 Thales helps address EDPB Recommendations for Schrems II

12 Conclusion

12 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](#).

This white paper describes how multinational companies can adhere to the European Data Protection Board's recommendations to address Schrems II ruling, using a trusted privacy framework provided by the industry leading data protection and trusted access management platforms from Thales.

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 address 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 \(EDPB\)](#) 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.

Data Protection Strategies for GDPR

If the assessment done at step 3 above reveals that GDPR transfer tools are not effective, then it is required to put the appropriate supplementary measures discussed in step 4 of the EDPB guidelines.

EDPB suggests multiple supplementary measures such as contractual, organization, or technical. Only technical measures are capable of addressing the data transfer challenges that arise from access to the data by public authority of third country outside EU.

Encryption is a powerful tool that is presented as one of the technical measures in the EDPB guidelines. Encryption renders the data illegible. Hence, even if public authority of the third country outside EU is able to access to the encrypted data, they will not be able to make sense of it without having access to the encryption keys.

What are BYOE, BYOK and HYOK data protection strategies?

Cloud providers increasingly offer their own encryption services to their customers. These services enable enterprises to secure data at rest with encryption across their cloud workloads and resources without compromise to business functionality.

In order to meet GDPR compliance mandates, data residency requirements, and best practices, enterprises using cloud provider encryption need to address additional requirements for managing encryption keys. These requirements are:

- Separating encryption key material storage from key usage locations
- Storing encryption keys within the sovereign boundary
- Customer management of key creation, rotation, deactivation, and destruction
- Separation of duties for key management
- Auditing of encryption key management, usage, and access

Bring Your Own Key (BYOK)

A growing number of cloud providers offer Bring Your Own Key (BYOK) services. In this model, the cloud provider performs the native encryption, but enterprise customers import their own keys to the cloud, which enables customer-controlled cloud key management.

Hold Your Own Key (HYOK)

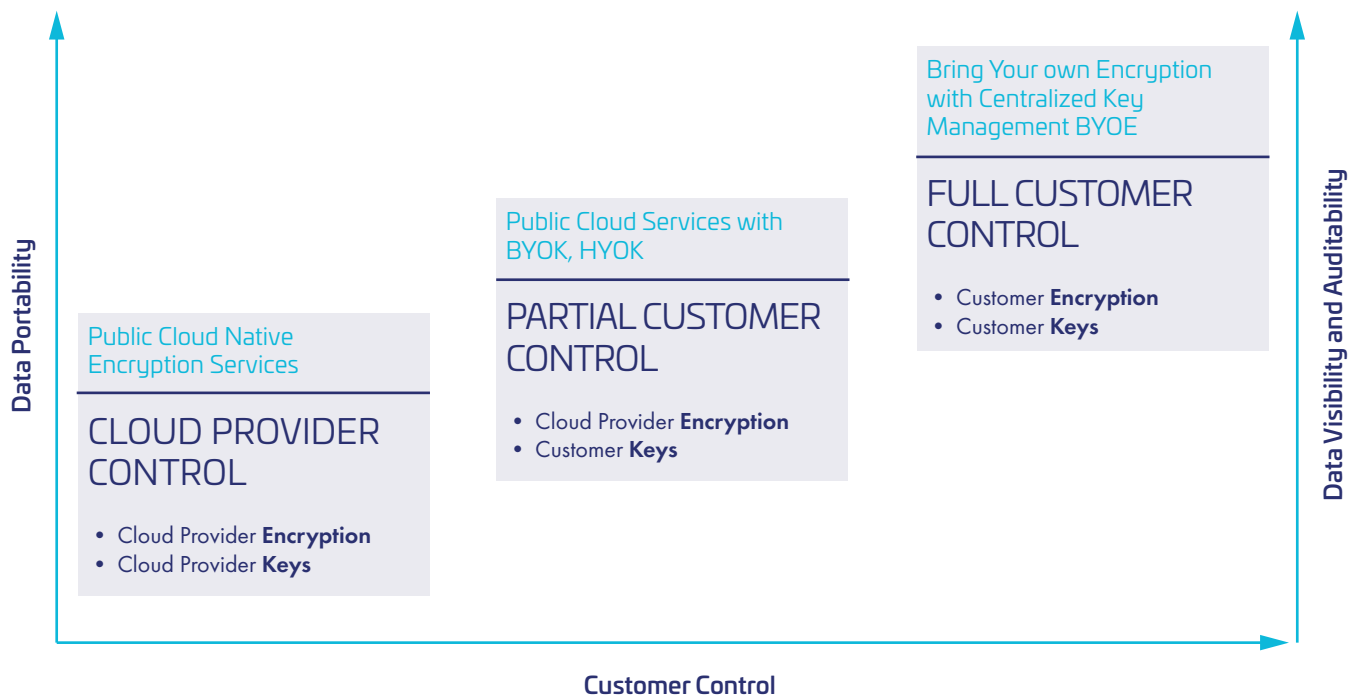
A few prominent cloud and SaaS providers have gone one step beyond BYOK by letting enterprise customers hold the key in their complete control. Whenever the cloud provider needs to access the encrypted data, it makes a request to the customer to get the cryptographic keys for the decryption operation. This feature is known as Hold Your Own Key (HYOK).

Bring Your Own Encryption (BYOE)

In Bring Your Own Encryption model, enterprises do not depend on cloud native encryption services at all. Instead they rely on the enterprise Key Management System (KMS) that they have been using in the private cloud/on premise environment. They protect their workload in the cloud by bring the same enterprise KMS and leverage the encryption agent to protect the data at application or file level.

Why BYOE is the right strategy to address Schrems II

Cloud data security might seem easy at first. Turning on the encryption for a public cloud provider is simple. But it's a multi-cloud world, and managing data security across multiple public clouds and different cloud storage options quickly gets complex. Bring Your Own Encryption (BYOE) lets your organization manage not only your encryption keys, but also the encryption process itself. It is considered to be the most secure option with the highest level of customer control for protecting data in multi-cloud environments. The chart below provides comparative analysis of the BYOK, HYOK and BYOE Strategies.

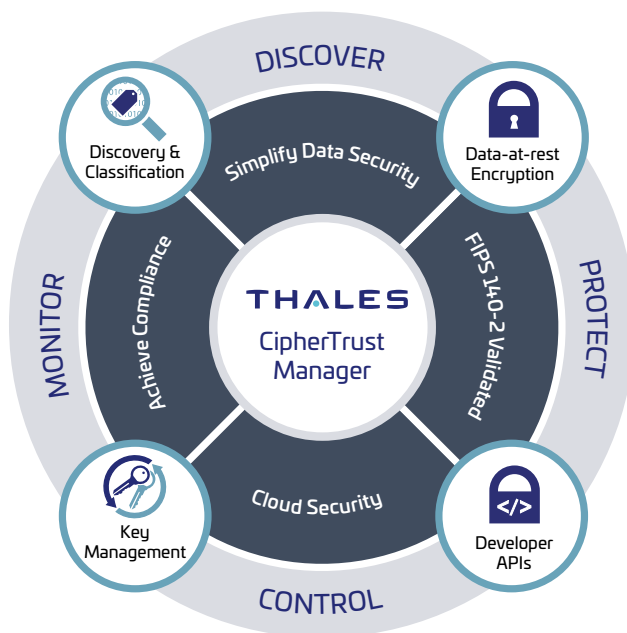


How Thales Can Help

Thales enables organizations to maintain compliance with GDPR and adhere to the European Data Protection Board (EDPB) recommendations for adopting the Schrems II ruling using the six-step plan for continually assessing and protecting global data flows.

Introduction to Discover, Protect, Control

Thales provides a unified data discovery, data classification, data protection, and unprecedented user and application access controls with centralized key management solution, with the CipherTrust Data Security Platform. Thales can help organizations to deploy BYOE and tokenization policies to protect sensitive data at rest in both EU (data exporter) and non-EU countries (data processors).



Discover:

Before data is transferred out of the EU, data exporters must be able to discover sensitive data records wherever they reside and classify them based on GDPR compliance requirements. CipherTrust Data Discovery and Classification enables organizations to get complete visibility into sensitive data on-premises and in the cloud, and then apply appropriate data protection measures as outlined by GDPR.

Protect:

Once the data exporter knows where their sensitive data resides, they can protect that data with encryption and tokenization solutions available in the CipherTrust Data Security Platform, before it moves to downstream data processors in other non-EU countries. The CipherTrust platform could be used in non-EU countries as well to provide adequate level of data protection, as in the EU countries. Thales High Speed Encryptions (HSE) protect data-in-motion with network independent encryption from site-to-site between EU and non-EU countries.

Control:

Every data security regulation including GDPR requires organizations to control access and monitor authorized/unauthorized access to data and encryption keys. CipherTrust Manager and CipherTrust Cloud Key Manager enable data exporters (EU countries) to centrally maintain control over their keys and access policies across on-premises and multi-cloud environments. Thales Luna Hardware Security Module (HSM), provides an high-assurance tamper resistant appliance that acts as a trusted anchor to protect master keys that encrypt data. Thales' SafeNet Trusted Access enables organizations to centrally control user access and provide single sign-on to all applications in the cloud and on-premises.

Bring Your Own Encryption (BYOE) Offered by Thales

There may be no “one size fits all” strategy for implementing BYOE. But, having a variety of options available on a single [CipherTrust Data Security Platform](#) from Thales, enables both data exporters and importers across EU boundaries, to implement encryption at the file/folder level, database level and application level, to satisfy EDPB recommendations to adhere to Schrems II. Thales also offers an extensive range of data protection and access management solutions to help enable GDPR compliance in the light of the Schrems II ruling.

Thales also offers an extensive range of data protection and access management solutions to help enable GDPR compliance in the light of the Schrems II ruling.

Transparent Encryption

[CipherTrust Transparent Encryption](#) delivers data-at-rest encryption, privileged user access controls, and detailed data access audit logging without re-engineering applications, databases, or infrastructure. Extensions are available for zero downtime data transformation and key rotation, simplified encryption advanced access controls for big data and SAP HANA. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

Database Encryption

[CipherTrust Database Protection](#) solutions integrate data encryption or tokenization for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, and IBM DB2 and Teradata databases.

Application Data Protection

[CipherTrust Application Data Protection](#) delivers crypto functions such as key management, signing, hashing, and encryption services through APIs, so that developers can easily secure data at the application server or big data node. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management.

Streamlined Tokenization

[CipherTrust Tokenization](#) offers both vaulted and vaultless and can help reduce the cost and complexity of complying with data security mandates such as PCI-DSS. The vaultless offering includes policy-based dynamic data masking. Both offerings provide tokenization services via RESTful APIs, while the vaulted offering has additional environment-specific APIs. Both offerings make it easy to add tokenization to applications.

Centralized Key Management

[CipherTrust Manager](#) enables organizations to centrally manage encryption keys, provide granular access control and configure data security policies. It manages key lifecycle tasks including key generation, rotation, destruction, import and export using developer friendly REST APIs. It is available in both virtual and physical form factors than can integrate with an embedded or external Hardware Security Module (HSM) for securely storing keys with the highest root of trust.

Hardware Security Modules

Cryptographic functions on [Luna Network Hardware Security Modules](#) (HSMs) and Luna Cloud HSM services on the Data Protection on Demand (DPoD) cloud-based platform enables organizations to securely manage, process and store crypto keys and functions inside a hardened, tamper-resistant, FIPS 140-2 validated appliances available as hardware for on-premises or in the cloud as a service on DPoD, or together as a hybrid solution.

Data Protection on Demand

The award winning [Thales Data Protection on Demand](#) (DPoD) is a cloud-based platform, providing a wide range of Luna Cloud HSM and CipherTrust Cloud Key Management services through a simple online marketplace. Just click and deploy the protection you need, provision services, add security policies and get usage reporting in minutes.

Network Encryption













[Thales High Speed Encryptors](#) (HSEs) provide network independent encryption (Layers 2, 3 and 4) for data in motion ensuring data is secure as it is transferred from site-to-site, or from on-premises to the cloud and back. Thales HSE solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — all at an affordable cost and without performance compromise.

Trusted Access Control

[SafeNet Trust Access](#) (STA) enforces access management at the login entry points protecting enterprise IT, web, and cloud-based applications from internal and external threats. STA utilizes policy-based conditional access, rigorous single sign-on (SSO), and universal authentication methods which prevent breaches, simplifies regulatory compliance and enables enterprises to migrate securely to the cloud.

Thales helps address EDPB Recommendations for Schrems II

The table below provides a summary of the applicable data protection and access control products from Thales that can help address the security measures recommended by EDPB to satisfy Schrems II ruling, including: Thales CipherTrust Data Security Platform, Luna Hardware Security Modules, Data Protection on Demand (DPoD), Thales High Speed Encryptors and SafeNet Trusted Access.

EDPB	Recommendations	Thales Supported Capabilities
Step 1	Know your data transfers	 Data Discovery and Classification
Step 4	Adopt supplementary measures	 Luna HSMs  Enterprise Key Management  Transparent Encryption  App Data Protection  Data Protection on Demand  Cloud Key Management  Database Protection  Tokenization  High Speed Encryptors (HSE)  SafeNet Trusted Access
Step 6	Re-evaluate at appropriate intervals	 Data Access Audit Logs

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 prove 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 data security solutions that can adequately protect global commerce. Since the fines of non-compliance could reach tens of millions of euros, it is incumbent upon companies to take Schrems II more seriously.

Thales offers the industry leading bring your own encryption, key management and access management solutions that make it easy for 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.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

