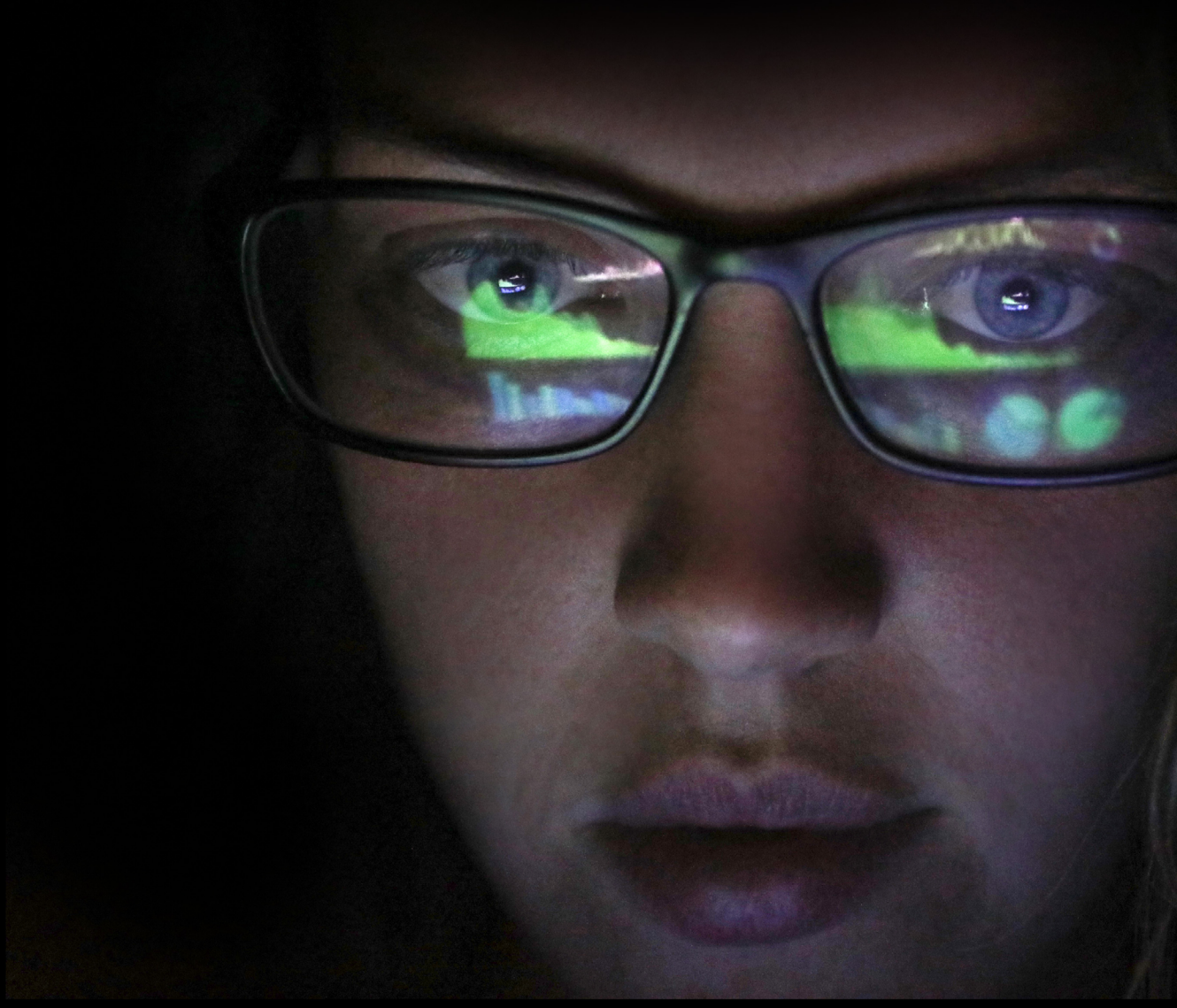
virtru

Who Holds the Keys to Your Data?

How to use your preferred cloud provider while maintaining data privacy & sovereignty.



The Digital Dilemma

Enterprises face a predicament: They want to leverage the productivity and security benefits of global cloud platforms but are concerned they will face conflicting legal obligations that put the privacy of customers at risk.

For example, a company based in Europe may find itself in a situation where it's required to hand over its customer data to the U.S. government.

Why? Because: (a) the leading cloud providers are predominantly U.S.-based and subject to various laws requiring cooperation with U.S. local and federal government entities, and (b) there is currently no multilateral privacy framework.

The absence of a global privacy framework has caused governments to take very different legal and policy approaches to data. For example, The European Union has adopted very strong privacy protections for its citizens, whilst the United States delegates some privacy issues to the individual state level (e.g., the California Privacy Rights Act, CPRA) while taking some actions at the federal level, such as the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act in 2018. In 2021, the European Data Protection Board issued a set of new recommendations for international data transfers, including what kinds of protections are sufficient for protecting private data.

Privacy has become a polarizing issue for these Western allies. The system of national and regional law continues to evolve, and companies need flexible tools to navigate this changing landscape.**Technology that puts the enterprise at the center of control can, and must be, a core part of the solution.** As the EU's latest recommendations emphasize, "the protection granted to personal data in the European Economic Area must travel with the data wherever it goes."

To understand how to address this complex issue, we need to understand the key components at play: The U.S. CLOUD Act, Schrems II, and the General Data Protection Regulation (GDPR).

U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act (2018)

Established: 23 March 2018

What is it? The U.S. CLOUD Act allows the U.S. government the ability to compel a U.S. cloud provider to hand over data regardless of where such data is stored, in any global geographic location (i.e., data stored on a Google server in Belgium would be subject to this law).

Why is it a concern?
Aside from the vast data protection and privacy issues handing data over to the U.S. government opens up, it also causes major operational headaches for organizations that need or want to do business in the global marketplace. While the U.S. is home to the vast majority of enterprise cloud providers—notably, Amazon, Microsoft, and Google hold 66% of the European cloud market share—it is uncertain how the U.S. tech industry will balance competing geopolitical demands in the absence of a formally adopted multilateral policy agreement to replace the Privacy Shield.

Some may choose to avoid the issue altogether and not adopt cloud-based technologies, potentially broadening the digital divide. Others may choose to only do business with EU or other non-U.S. cloud providers, fuelling the worrisome trend of isolationism and walled gardens that have sprung up around the globe.

Schrems II & the General Data Protection Regulation (GDPR)

Established: Schrems II was ruled on 16 July 2020 and GDPR came into effect 25 May 2018

What is it?

Schrems II is known as the ruling by the Court of Justice of the European Union (CJEU) that invalidated the EU-U.S. Privacy Shield Framework due to concerns around U.S surveillance practices. Fair or unfair, the reality is that the 2013 Edward Snowden revelations continue to cast a long shadow over U.S. surveillance practices.

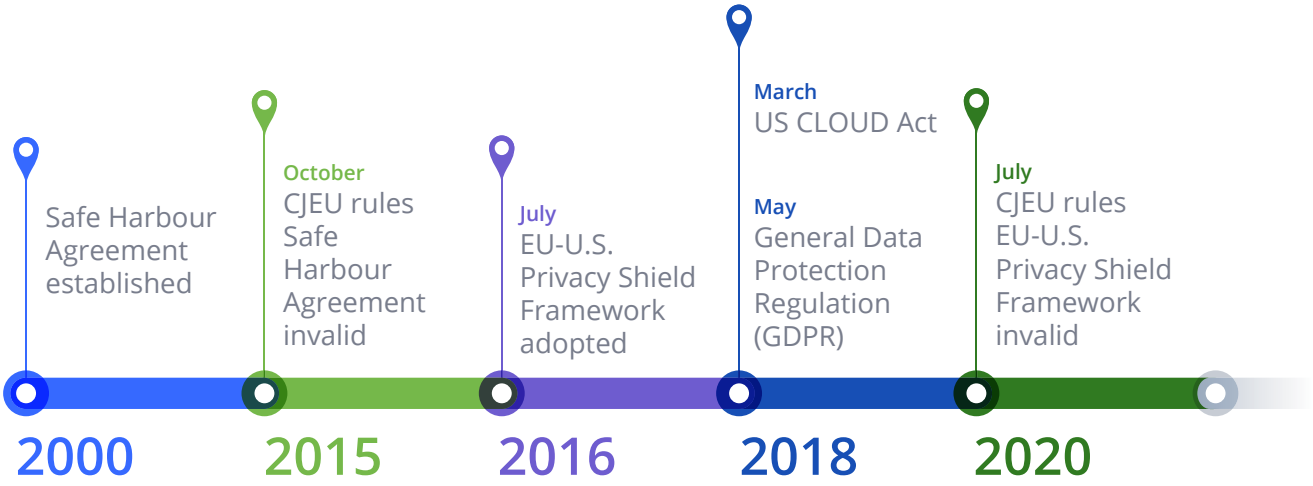
GDPR is an EU regulation that governs the mechanisms under which the transfer of personal data outside the EU can be lawful. Its primary aim is to give individuals (and companies for their employee and customer data) control over their own data, how it is being used, under what timeframe, and for what purpose.

What does this mean?

Schrems II addressed the validity of both the Privacy Shield and standard contractual clauses (SCCs). Whilst transfers of personal data on the basis of Privacy Shield are now unlawful, on a case-by-case basis and with additional stringent controls observed, SCCs remain a valid, legal mechanism for data transfers. Data controllers or processors (here, for our purposes, “cloud providers”) that intend to transfer data based on SCCs, must now deploy a transfer mechanism to ensure the data subject is granted a level of protection equivalent to that guaranteed by GDPR.

The Changing Landscape of EU-U.S Data Regulation

The global data privacy landscape has undergone a substantial shift over the past 20 years, as data sharing has become ubiquitous. Here are some of the key regulation milestones that have shaped our current environment.



Safe Harbour Agreement is established - 2000

- Designed to ensure data transfers between the EU and the U.S. complied with the European Data Directive 1995 (predecessor to General Data Protection Regulation (GDPR)

CJEU rules Safe Harbour Agreement invalid - 6 October 2015

- A result of a case against Facebook (Schrems I) brought by Max Schrems, an Austrian Privacy advocate, who challenged the transfer of his data (and the data of EU citizens' generally) to the U.S. by Facebook, which is incorporated in Ireland.

EU-U.S. Privacy Shield Framework is adopted - 12 July 2016

- Designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the U.S. in support of transatlantic commerce.

US CLOUD Act comes into effect - 23 March 2018

- Allowed U.S. law enforcement authorities to request personal data from U.S.-based technology companies regardless of the data's location.

General Data Protection Regulation (GDPR) comes into effect - 25 May 2018

- Designed to give EU citizens more control over their personal data and to simplify rules for organizations that operate within, and those that do business with, EU member states.

CJEU rules EU-U.S. Privacy Shield Framework invalid - 16 July 2020

- Known as Schrems II, this decision rejected the framework based on concerns around U.S. surveillance practices.

How Privacy and Cloud Collaboration Can Coexist with End-to-End Encryption

Given the market dominance of U.S. cloud and software solution providers (i.e., organizations that fall under the scope of the U.S. CLOUD Act), most companies competing in the EU that leverage cloud technologies and collect consumer data (i.e., organizations that fall under the scope of the Schrems II decision) must face the issue of U.S. vs. EU regulations head-on as they operate day to day.

Fortunately, there is a solution for those businesses—one that enables full participation in the global economy, maintains the benefits of the public cloud, and provides complete control over data access.

In November 2020, the European Data Protection Board (EDPB) adopted guidance clarifying that ***end-to-end encryption is an effective measure to enable both cloud adoption and EU data sovereignty requirements***, which are often viewed as the global privacy gold standard.

End-to-end encryption enables enterprises to:

- Adopt global cloud services while meeting data sovereignty requirements.
- Protect privacy rights of customers.
- Maintain full control of the data with which they have been entrusted.
- Ensure that competitors, foreign governments, and other entities who should not have access cannot gain access to their proprietary or otherwise sensitive information.

In essence, companies competing in the EU can pair stringent security controls offered through encryption technology with SCCs, ensuring compliance with European law post-Schrems II while offering a managed path to authorized access for U.S. government agencies and other entities. This is where Virtru can help.

Virtru's End-to-End Encryption Enables Secure Data Sharing and Data Sovereignty in the Cloud

Virtru has adopted an approach to data security that prioritizes privacy and control that is fully managed by their customers—otherwise known as data sovereignty. The Virtru platform provides end-to-end encryption that ensures your data—and your customers' data—remains encrypted and unreadable (in line with the EDPB guidance) even in the event of the U.S. CLOUD Act being activated.

How?
Virtru's solution is cloud infrastructure- and provider-agnostic, crypto-agile and implemented end-to-end as a default. Encrypted key management options ensure that no entity—including cloud vendors—is able to access the data without obtaining consent from the data owner, who has the sole ability to grant access through decryption.

In a nutshell, Virtru supports global collaboration through compliant, cross-border data flows by ensuring:

We are already helping organisations maintain control of their data:

Major-European Retailer Requires Additional Security to Ensure True Privacy of Sensitive Data from Cloud Provider

Read Case Study

1. Data can be stored on any cloud solution, including those offered by U.S.-based providers including commercial off-the-shelf solutions from Google, Microsoft, and Amazon.
2. Data is wrapped in a layer of protection (encryption) that can only be unlocked by the designated customer or recipient. While the data is still accessible, it remains encrypted and unreadable.
3. The keys that unlock that protective layer are managed outside of the cloud solution. Virtru offers the capability to store the encryption keys—the core of the encryption mechanism—on premise or in a private cloud that is solely owned and managed by the customer, thereby achieving data sovereignty.

In an ever-shifting policy landscape, Virtru remains focused on what matters: **ensuring data sovereignty, empowering end customers with unique control of their data, and fostering trusted collaboration across borders.**

Want to see how Virtru's end-to-end encryption can protect your company's proprietary data, everywhere it's stored and shared? Contact us for a demo today.

virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of encryption solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 6,000 customers trust Virtru for data security and privacy protection.