ForgeRock®

WHITEPAPER

Enable Schrems II Alignment with ForgeRock® Identity Cloud

Executive Summary

The evolution of the transatlantic data sharing regime between the European Economic Area (EEA)[1] and the United States (U.S.) has left many cloud vendors scratching their heads in frustration. The decision by the Court of Justice of the European Union (CJEU) in July 2020 to invalidate the Privacy Shield Framework has increased regulatory risks associated with cross-border data flows. It has also increased compliance costs while creating uncertainty surrounding data residency, privacy, and, ultimately, trust among consumers of digital services globally.

Modern identity and access management (IAM) solutions can help you to address some of these risks and work towards aligning with the Schrems II ruling. The **ForgeRock Identity Cloud** provides security and privacy by design through full tenant isolation, and robust data encryption to ensure that both the storage and transmission of data is in line with the principles of Schrems II. These capabilities help you reduce regulatory risks and compliance costs, while strengthening consumer privacy and trust. The ForgeRock technology stack also allows you to benefit from the comprehensive SaaS capabilities while retaining data within an EU region of choice or even on-premises, where this is required.

The Importance of Transatlantic Data Flows

Cross-border data flows are critical to the modern global digital economy. They enable governments, businesses, and people to share information for research, commerce, and the facilitation of cross-border services and international trade. Nowhere is the flow of data more prominent than between the EEA and the U.S. According to the **U.S. Bureau of Economic Analysis**, trade in information and communications technology (ICT)-enabled services was worth $264 billion U.S. dollars in 2020. This market includes data shared for the purposes of discharging financial services, business services, as well as research and development collaboration, distribution of software (worth $10.8 billion in 2019), and provision of cloud computing and data storage (worth $1.7 billion in 2019).

The rise in ICT trade has been further accelerated by the rapid adoption of cloud computing and the increasing role that these services play in driving digital transformation. The onset of the COVID-19 pandemic and advent of the "**new normal economy**" has turbo-charged the pace of digital transformation across all industries. Research from **Statista** shows that over 65% of EEA companies transfer data outside the EU. Secure flow of data has never been more important for consumers, businesses, and governments.

> **"The United States and the EU share an extensive, highly integrated trade and investment relationship. Cross-border data flows between the United States and the EU are the highest in the world."**
>
> **U.S. Congressional Research Service**

Evolution of the Transatlantic Data-Sharing Regime

The International Safe Harbor Principles came into effect in 2000 with the purpose of facilitating cross-border data flows between the U.S. and the European Union (EU). They comprised specific principles that gave EU data controllers transparency into and control over the onward transfer of their data to data processors[2] (including third parties) resident in the U.S., placing obligations on these entities to safeguard data integrity and security.

The International Safe Harbor Principles were invalidated in October 2015 by the **CJEU Schrems I ruling**, which was brought by the privacy activist Maximillan Schrems against Facebook in the Irish Republic[3]. Mr Schrems had claimed that his personal data had been transferred from Facebook servers in Ireland to servers based in the U.S. without providing "adequate protection" from unauthorized access by surveillance agencies. The Schrems I ruling affected more than 4,500 companies operating within the Safe Harbor Principles, and led to the advent of the successor EU-U.S. Privacy Shield Framework in July 2016.

The EU-U.S. Privacy Shield Framework reinforced the dispute resolution mechanisms and was forged on the written assurances of the executive branches of the U.S. government that "adequate protection" would be provided to prevent disclosure of personal data owned by EU consumers to third parties outside the EEA jurisdiction, further solidifying the principles laid down by the General Data Protection Regulation (GDPR). The EU-U.S. Privacy Shield Framework was subsequently invalidated in July 2020 by the **CJEU Schrems II ruling** brought once again by Maximilian Schrems against Facebook in the Irish Republic[4].

The ruling stated that the EU-U.S. Privacy Shield Framework did not provide adequate enforcement for GDPR provisions and, in particular, protection of personal data owned by EEA consumers outside its borders. Responding to the ruling, the European Data Protection Board (EDPB) issued a set of FAQs[5] that placed the responsibility for undertaking transfer risk assessments (TRAs) on **individual organizations**.

In reality, the Schrems II ruling had also exposed the risks inherent in the transatlantic cross-border data sharing, inadvertently driving data localization while increasing the strategic importance of data residency, encryption, and access management. On March 25 2022, the U.S. and the European Commission released a **joint statement** announcing the in-principle agreement of the Transatlantic Data Privacy Framework, or "Privacy Shield 2.0." It is as yet unclear what this new framework will mean for businesses worldwide.

The Role of IAM in Achieving Schrems II Compliance

IAM technology is becoming more pervasive in shaping how consumers, workforce, and "things" connect with the digital world. Rapid acceleration of digital transformation across all industries worldwide has driven IAM architecture to the core of the tech stack across many IT ecosystems. This has, in turn, led to the proliferation of both personal and non-personal identity data, which can be stored locally on-premises, in the cloud, or across hybrid IT infrastructures.

The evolution of the transatlantic data sharing regime has placed an onus on organizations to put in place appropriate safeguards, access controls, and operational procedures to ensure that identity data is stored securely and, where/when needed, transmitted in accordance with the Schrems II ruling and the standard contractual clauses (SCCs[6]). Modern IAM technology is becoming increasingly critical to helping organizations ensure they are compliant and able to continue scaling across global markets. So, what should you be looking for in your IAM to help you align with Schrems II?

1. **Secure data storage and flexible residency:** Modern IAM solutions can be deployed on-premises, across any cloud, or in hybrid IT environments. This means that *personal identity data*[7] can **potentially** be stored and/or moved between data centers resident in different geographical locations.
2. **Robust data encryption at rest:** Modern IAM solutions leverage cryptographic techniques and technologies to protect *personal identity data*, thus preventing unauthorized access. Aligning with Schrems II therefore places a responsibility on you for putting in place adequate arrangements for the encryption of personal identity data at rest, whether stored on-premises, in the cloud, or within a hybrid IT infrastructure
3. **Robust data encryption in transit:** Modern IAM solutions further enhance standard security protocols (such as HTTPS, TLS) by allowing organizations to put in place controls for how, when, and by whom *personal identity data* can be transmitted.

How ForgeRock Addresses Schrems II Compliance

The ForgeRock Identity Cloud helps you align with the Schrems II ruling and the SCCs through:

1. Data sovereignty with regional isolation

- The ForgeRock Identity Cloud provides you with access to the broadest IAM cloud footprint, spread across 17 regions worldwide, including six based in the wider European region.[8] This distribution gives you the flexibility to ensure that *personal identity data* can reside within EEA borders. It also future-proofs your IAM investments against possible changes in the transatlantic data-sharing regime, allowing you to adjust your data residency arrangements as needed.
- The ForgeRock Identity Cloud leverages the native physical and network security features of the **Google Cloud Platform** (GCP), based on industry-leading security policies to maintain the infrastructure, services, and physical access policies and procedures. With GCP, you have the assurance that *personal identity data* is stored and processed in line with industry-leading best practices and enterprise-grade security.
- The ForgeRock Identity Cloud is built to **provide security and privacy by design** through complete tenant isolation (see figure 1)[9], meaning there is absolutely no co-mingling of data. Each customer environment is self-sufficient, sovereign, comprising a distinct GCP namespace environment that runs a distinct copy of the service code under dedicated identities, and provides dedicated storage for customer data and secrets that only the customer can access.[10] This isolation provides you with the assurance that *personal identity data* is containerized, secure, and accessible without undue interference of "noisy-neighbors" (i.e., other cloud customers) since no one else is sharing the same tenant.
- Because the ForgeRock Identity Cloud provides security and privacy by design through a full tenant isolation architecture, it ensures that your *personal (customer, workforce, "non-human") identity* data is both **stored** and **processed** in one unified tenant. Selecting one of the ForgeRock cloud regions in the EEA region therefore prevents you from storing the data in one tenant and then having to ship this outside the said region for processing. The ForgeRock Identity Cloud provides you with dedicated processing within the isolated tenant of your choice.

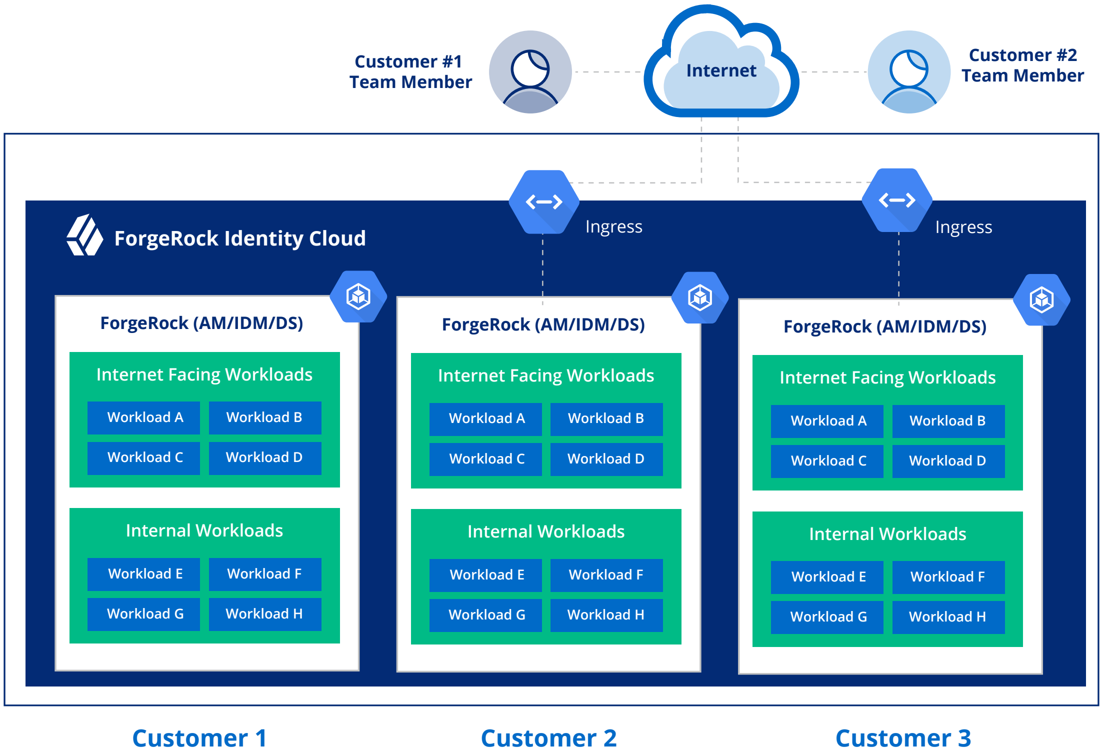

Figure 1: ForgeRock Identity Cloud security and privacy by design-driven architecture.

2. Data encryption at rest

- The ForgeRock Identity Cloud leverages the layers of cryptographic technologies and techniques employed by GCP. This secures **all** *personal identity data* at rest held in GCP data centers resident in a location of your choice, mitigating the risk of unauthorized access.
- The GCP encryption model for data at rest (see detailed **GCP whitepaper** for full detail) splits data into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) encryption keys that are exclusively stored and used inside Google's central Key Management Service (KMS). All data stored in Google Cloud is encrypted at the storage level using AES256.
- GCP uses several layers of encryption to protect data. Using multiple layers of encryption adds redundant data protection and allows GCP to select the optimal approach based on application requirements. This partition of data, each using a different key, means the "blast radius" of a potential data encryption key compromise is limited to only that data chunk (see figure 2).

3. Data encryption in transit

- The ForgeRock Identity Cloud leverages the layers of cryptographic technologies and techniques employed by GCP. This secures *personal identity data* in transit while it flows over public (such as the internet) and/or private networks (such as a corporate LAN or WAN), mitigating the risk of unauthorized access.
- The GCP data encryption model for data in transit (see full **GCP whitepaper** for detail) encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted.
- Depending on the connection being made, Google applies default protections to data in transit. For example, the Transport Layer Security (TLS) protocol is often used to encrypt data in transit for transport security.

4. Data processing capabilities and arrangements

- ForgeRock employee access to the ForgeRock Identity Cloud is strictly controlled. This includes tight role-based controls ensuring that only authorized ForgeRock employees have access to customer data. All access to the ForgeRock Identity Cloud is routinely audited.
- The ForgeRock Identity Cloud Global Support Model operates a "follow-the-sun" resourcing model for 24/7 deployment support scenarios. This means that cloud infrastructure-level support (via ForgeRock and GCP) and application-level support may be provided by a Support Engineer outside the EEA borders. All customer logs needed to provide both infrastructure-level and application-level support, however, stay in the region of customers' choice.
- The ForgeRock Identity Cloud maintains complete tenant isolation, meaning your data will never be co-located within a data store used by another ForgeRock customer. When deploying a cloud environment, you can choose the region in which the tenant and tenant data will reside. Your data will be maintained in this region at all times. For backup copies, data will be stored in a backup format in another location within the same region to maintain disaster recovery (DR) and business continuity (BC) best practices. Backups are stored in multiple zones within the region, separated by significant physical distance.
- The GCP backup system ensures that data remains encrypted throughout the backup process. This approach avoids unnecessarily exposing plaintext data. The backup system further encrypts each backup file with its own data encryption key (DEK), derived from a

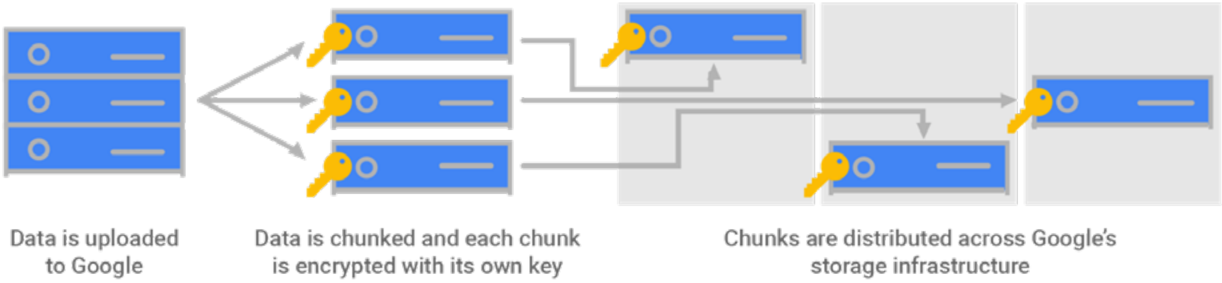
Data is uploaded
to Google
Data is chunked and each chunk
is encrypted with its own key
Chunks are distributed across Google's
storage infrastructure

Figure 2: GCP encryption model for data at rest

key stored in Google’s KMS plus a randomly generated per-file seed at backup time. Another DEK is used for all metadata in backups, which is also stored in Google’s KMS (see figure 3). This backup would be needed only if all distributor instances were to go down at once; for example, in a global restart. Fewer than 20 Google employees are able to access the physical encryption key safes.

5. “Break-glass” support

- The ForgeRock Identity Cloud Global Support Model includes a “break-glass” operational procedure, which you may decide to activate during emergency events. This procedure includes a “break-glass account” for use if ForgeRock has lost access to the service, or is at imminent risk of losing access. The account is not used for any operational needs, and is only used to grant ForgeRock Support Engineers temporary privileges for the purpose of fixing the critical issue at hand. All privileges are temporary and are removed once the issue is resolved. Use of the “break-glass account” will trigger a security alert.
- The security alert triggers a “customer assent process” which allows you to:
  - Approve controlled access for a ForgeRock Support Engineer within your tenant
  - Monitor all actions of a ForgeRock Support Engineer within your tenant
  - Revoke privileges for a ForgeRock Support Engineer to access your tenant at any time

6. Extend on-premises deployments

The ForgeRock Identity Cloud is kept current with new product features and enhancements, giving you access to the best in-class identity SaaS capabilities. If you are not yet ready to fully transition to the cloud, you have the option of extending your on-premises deployment through ForgeRock Directory Services, while benefiting from the connected capabilities offered by the ForgeRock Identity Cloud.

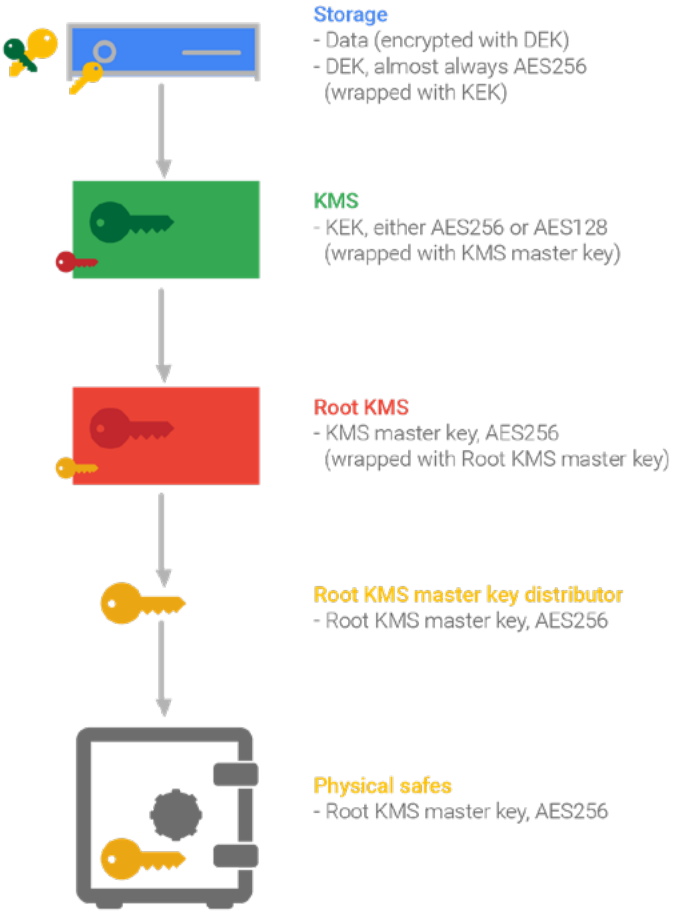
Storage
- Data (encrypted with DEK)
- DEK, almost always AES256 (wrapped with KEK)
KMS
- KEK, either AES256 or AES128 (wrapped with KMS master key)
Root KMS
- KMS master key, AES256 (wrapped with Root KMS master key)
Root KMS master key distributor
- Root KMS master key, AES256
Physical safes
- Root KMS master key, AES256

Figure 3: GCP encryption hierarchy

In addition to the above, the ForgeRock Privacy Team will help you facilitate your alignment with the Schrems II ruling by providing you with access to the following resources during your buying journey/pre-deployment:

- Description of our **data processing activities**
- GDPR-compliant **privacy terms**
- A **list of subcontractors** who support our global service delivery model and who are bound to suitable terms
- Access to TRAs for our data processing activities undertaken in the U.S., Singapore, and Australia (available on request)

Summary

The ForgeRock Identity Cloud helps you align with Schrems II ruling, while accelerating your transition to the cloud. The ForgeRock Identity Cloud provides you with a layered defense-in-depth approach built on security and privacy by design, full tenant isolation, data sovereignty with regional isolation, and data encryption at rest and in transit. This layered approach help you to:

- Reduce regulatory risks associated with Schrems II
- Reduce compliance costs associated with Schrems II
- Strengthen consumer privacy and trust

[1] The EEA extends the European Union Single Market to the active members of the European Free Trade Association (Iceland, Liechtenstein, Norway).

[2] **Formal EU definition** of a data processor.

[3] The case was initially brought forward with the Irish Data Protection Commissioner, and subsequently referred to the CJEU via Irish High Court.

[4] Ibid

[5] Followed by the publication of the **strengthened SCCs and guidance** in June 2021. The EC formally adopted the updated SCCs and guidance in June 2021, with these coming into effect from September 2021.

[6] SCCs for **international transfers**. SCCs for **controllers and data processors**.

[7] Includes, but is not limited to: (i) name, (ii) email address, (iii) IP address, and (iv) user ID. For more information see the ForgeRock Identity Cloud Data Privacy Data Sheet.

[8] These include data centers in London, Belgium, Netherlands, Germany (Zurich, Frankfurt), Finland. For more information see **ForgeRock Backstage**.

[9] This is a fully patented technology. For more information, see the **ForgeRock Identity Cloud Security whitepaper**.

[10] In a true data isolation model, every customer setup is a discrete deployment, separate and apart from any other customer. Data is stored in a containerized Kubernetes cluster accessible only from the tenant's cloud. One customer's instance never interferes with another's, and there are no shared resources to compete for..

Further Information

If you would like to discuss any aspect of ForgeRock's technical and organizational measures around our product's privacy controls, please contact ForgeRock's Chief Privacy Counsel at **privacy@forgerock.com**.

About ForgeRock

Follow Us

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that delivers modern and comprehensive identity and access management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than 1300 global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com**.

ForgeRock