



EQUINIX  
SMARTKEY™

Powered by  Fortanix®

ACCELERATE GDPR  
COMPLIANCE WITH SMARTKEY™:  
CLOUD-BASED KEY MANAGEMENT  
AND CRYPTOGRAPHY SERVICE

# UNDERSTANDING GDPR BEYOND BUZZWORDS, AND 4 PRACTICAL STEPS TO MEET COMPLIANCE

EQUINIX WHITE PAPER

# INTRODUCTION

The General Data Protection Regulation (GDPR) is designed to provide better privacy and security to European citizens and went into effect on May 25, 2018. In today's data-centric world that is marred by constant data breaches and chilling personalization of the web, individuals have been left wondering how their data is used and misused. GDPR can be best thought of as a legal framework to enforce common-sense, effective and practical data protection for personal data.

GDPR can be best thought of as a legal framework to enforce common-sense, effective and practical data protection for personal data.

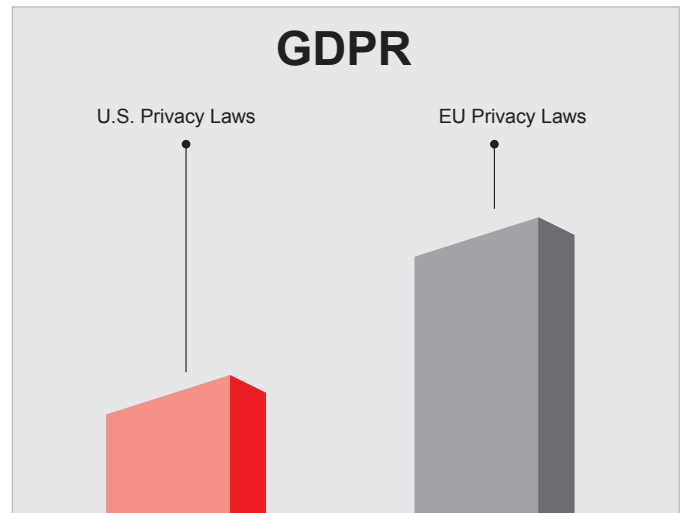
Codifying these steps, however, can lead to a complex set of legalese, and GDPR is no exception. As security and risk management (SRM) leaders rush to understand the impact of GDPR on their organizations, there are practical steps to take to meet the compliance requirements. Although GDPR is a European regulation, it affects customers and organizations beyond Europe. Even organizations without any European presence must adhere to GDPR if they process European customers' data. Additionally, GDPR may set a new standard for protecting customers privacy and start a trend in data laws.

# EDWARD SNOWDEN AND PRIVACY

To better understand the context behind GDPR, it's helpful to review the history of data protection laws in the United States (U.S.) and European Union (EU). As a critical component of privacy and human rights, the EU adopted the Data Protection Directive in 1995, which restricted personal data of European citizens outside EU to only those countries that guaranteed a certain level of data protection. The "Safe Harbor Principles" allowed U.S. organizations to self-certify, after which the EU would recognize them as adequate to offer the protection required by the directive. The Safe Harbor Decision turned out to be a landmark decision and simplified operations of U.S.-EU organizations by facilitating smooth transatlantic data movement. It made sense, as U.S. and EU share a great deal of cultural values from democracy to human rights to rights to privacy.

Then, global surveillance procedures were publicized, along with the release of documents by Edward Snowden. The ensuing reports uncovered a vast number of government programs accessing personal data of the general population. In light of this, and in response to a complaint from an Austrian citizen, the EU Court of Justice declared Safe Harbor invalid on October 6, 2015. Exporting the personal data of EU citizens to the U.S. would compromise **"the essence of the fundamental right to respect for private life."** Since the invalidation of Safe Harbor, the EU-U.S. Privacy Shield has been created as another

framework to facilitate data transfer between the two regions. But, the situation remains murky at best. The European Data Protection Supervisor noted that "the Privacy Shield, as it stands, is not robust enough to withstand future legal scrutiny before the [European] Court." At the same time, the computing background of the 1990s against which the Data Protection Directive was crafted had changed considerably, and a new framework was needed.



# WHAT'S GDPR? A LEGAL FRAMEWORK FOR COMMON-SENSE DATA PROTECTION

General Data Protection Regulation (GDPR) was proposed by various EU institutions, including the EU parliament and EU commission, as a single unified regulation to protect the data of all individuals living within the EU, regardless of where the data is collected, stored, or processed. While the GDPR text runs into hundreds of pages, most of the requirements include common-sense, if not obvious, ways of empowering customers to control their privacy and access to their data. Other parts of the regulation acknowledge the global nature of e-commerce today and increased complexity of organizations operating in multiple jurisdictions.

## **Binding regulation and big fines**

Unlike the previous Data Protection Directive, GDPR is a regulation, meaning it is a binding legislative act. Also, organizations can be fined up to 4% of their global revenue, or €20M, whichever is the maximum. Clearly, regulators have done their job seriously.

## **Wide applicability**

GDPR applies to any data that can be used to directly or indirectly identify a person. This includes financial data, photos, home addresses, medical information, social media, IP address, etc., whether they relate to customers' private, professional, or public life.

## **Clear consent**

Customers must be presented with clear, easy-to-understand, and easy-to-reject options before they consent to organizations collecting their data. No more hiding behind legalese that very few customers read.

## **Need to know**

Organizations keep and process the data only for the legitimate business needs and legal purposes.

## **Location does not matter**

As organizations collect data at global scale and use cloud computing distributed across multiple data centers and nations, GDPR does not consider where the data is processed or who processes it.

## **Right to be forgotten**

Customers can request erasure of their data based on multiple factors including GDPR non-compliance, termination of business, etc.

## **Data portability**

Customers are able to transfer their personal data from one processor to another.

## **Privacy by design and deliberate actions**

Organizations are to embrace the principles of privacy by design in their practices by splitting various roles (controller—one which defines how data should be processed and by whom vs. processors—potentially third-party organizations processing data as instructed by the controller), applying pseudonymization as soon as possible to reduce risk scope, creating a new internal role (data protection officer) to oversee compliance, etc.

## **Quick and simplified data breach reporting**

Data breaches must be reported within 72 hours, but contacting just the authority in the affected citizen's country may be sufficient. Thus, organizations don't need to contact multiple authorities. Again, regulators have adopted a very reasonable workflow.

This document does not offer any legal advice, and organizations should solicit feedback from expert legal advisors on their exact situation. For more details and further clarity, refer to publications including [Toolkit: General Data Protection Regulation Readiness Schedule](#) and [GDPR Clarity: 19 Frequently Asked Questions Answered](#).



# 4 STEPS TO GDPR COMPLIANCE

Meeting GDPR takes more than just technology. Corporations first need to adopt a new culture, organizational awareness and privacy-first mindset before using a centrally controlled and logged system to enforce access control. Sensitive data should only be collected from customers for a legitimate business need.

## Process, organizational, cultural

### 1 Understand your exposure

Driven jointly by legal and business unit leaders

- Identify programs and products affected by GDPR
- Establish process for user consent and business need for data
- Establish workflow for data access, retention and erasure
- Appoint data protection officer (required in some cases)



1

### 2 Continuous compliance

Driven by data protection officer or business unit leaders

- Identify data processors and their responsibilities
- Establish a post-breach strategy (informing required authorities and users)
- Monitor data breaches
- Drive awareness about GDPR, especially in product teams and operations



2

## Product and technology

### 3 Embrace privacy by design

Driven by information technology, engineering and business unit leaders

- Use technology to reduce exposure by pseudo-anonymizing
- Include unified access control for all sensitive data
- Encrypt all relevant data and integrate data erasure techniques
- Integrate a data access audit trail to corporate SIEM or similar platforms



3

### 4 Use encryption and key management for data privacy

Driven by information security professionals in collaboration with business unit

- Encrypt all sensitive data with a central key management policy
- Use solutions that works seamlessly across multiple data centers and clouds
- Meet data portability compliance requirement
- Audit all accesses in a secure, tamper-proof log



4

# TECHNICAL FRAMEWORK FOR DATA CONTROLLER AND DATA PROCESSOR

A data controller is an entity in an organization that determines what personal data is collected and processed and for what purposes. The data controller decides who has access to the data and for how long. Best practices recommend that data controller use Access Metadata for every piece of personal data. Access Metadata is the control layer between the data controller and the data processors to meet GDPR requirements about data audit, control and erasure. The data processor is an entity that processes the personal data according to rules set by the data controller. A typical large organization may have multiple data processors in multiple locations.

## Access Metadata is a collection of critical information organizations need for GDPR compliance:

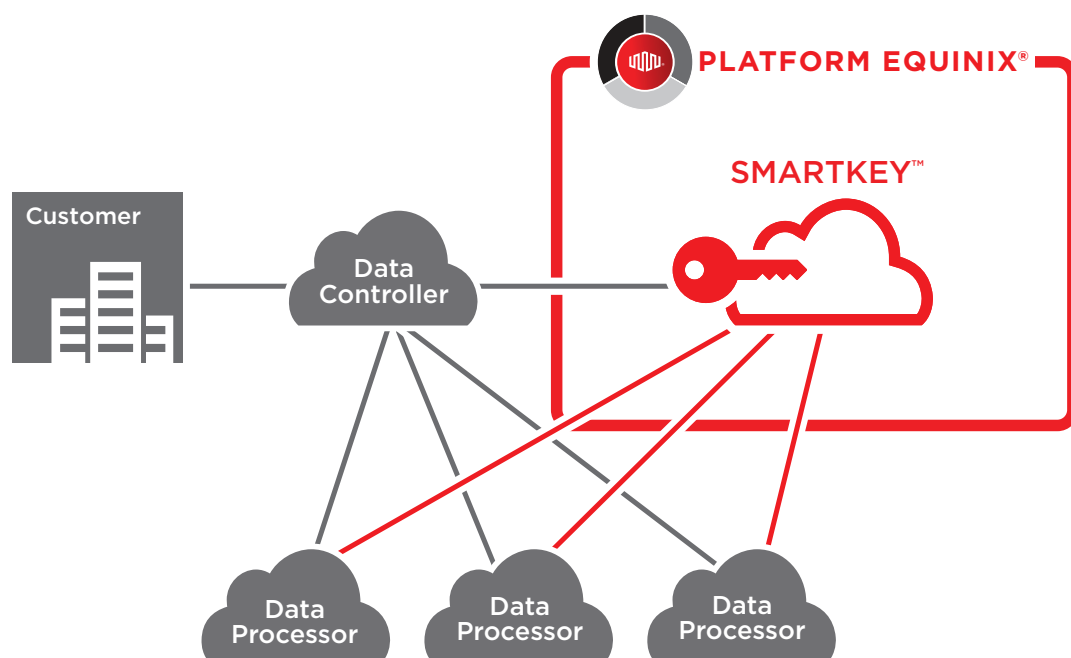
- A record of the customer consent in collecting the data
- A list of data processors and applications which have access to the data
- Directives on how the data processors can use the data

## Additionally, Access Metadata has the following capabilities:

- It allows the customer to request data erasure
- It allows the data controller to revoke a data processor's access
- It maintains a centralized audit log of all accesses
- It may have a time bomb for automatic deletion of personal data at a predetermined time in future

One of the basic tenants of GDPR is that the requirements don't depend on where data is processed. By specifically creating a control layer in the form of Access Metadata, organizations can centrally enforce the rules of data access.

## Simplify Compliance with SmartKey



Organizations need to categorize their data and create a set of rules to follow while processing their customers' personal data. Once the data access rules have been defined, organizations can encrypt the personal data with keys managed by Equinix SmartKey, powered by Fortanix, Key Management and Cryptography Service to help meet GDPR requirements.

SmartKey offers HSM security with software flexibility and is available in various form factors, including HSM as a Service (HSMaaS) for easy use. Encryption keys can be securely generated, stored, distributed, revoked, imported, exported, and managed within SmartKey. The encrypted data can then be made available to all data processors across the globe according to existing data architecture. Additionally, the Access Metadata can be sent to SmartKey. Thereafter, SmartKey will allow the decryption of data only if the requested action is allowed by the Metadata.

SmartKey is available globally as an SaaS with telecom-grade service availability. Thus, data processors in various clouds can communicate with SmartKey and decrypt data as needed. On the other hand, data controllers can continue to control the access rules with the Metadata. One of the benefits of using SmartKey, which leverages Intel® SGX, is that keys cannot be used without proper authorization and without creating an immutable audit trail. This strong assurance reduces compliance risk and provides organizations with a record in the form of the audit trail.

The following SmartKey capabilities help address GDPR requirements:

- **Encryption:** SmartKey can encrypt personal data and mark the keys exportable. Such keys can only be used according to rules set in Metadata
- **Tokenization and pseudonymization:** Certain kind of personal data should be tokenized or anonymized for better privacy. SmartKey offers these features built-in without additional cost
- **Tamper-proof central audit log:** SmartKey logs every action performed by data processors and the data controller into a centralized audit log
- **Proof of data erasure:** If a customer requests data erasure, SmartKey can delete the decryption key. Such a deletion is irreversible and is logged into the central audit log. Organizations can be assured that data cannot be used once the key has been deleted
- **Access revocation:** The data controller may want to revoke access of a data processor for various reasons, such as workload migration, business completion, etc. SmartKey provides a one-touch solution for data controllers to revoke such access
- **Automatic real-time synchronization:** All the keys, audit log and Metadata are synchronized across the SaaS service
- **Low-latency connection with CSP:** SmartKey is hosted in Equinix data centers around the globe, which offers the lowest latency to the processors located in major public cloud providers
- **Supports both traditional and new applications:** By providing a variety of traditional interfaces such as PKCS#11, CNG, JCE, EKM, and KMIP, existing applications can use SmartKey. Additionally, new applications can use native RESTful APIs for easy integration.

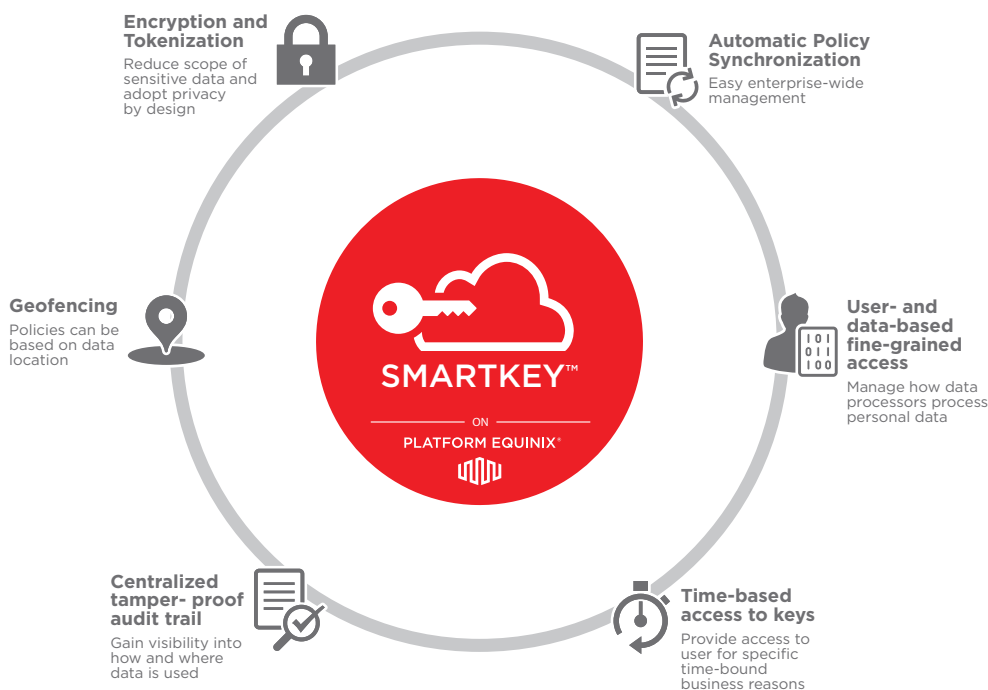
There is no magic formula that prescribes “use this software to achieve complete GDPR compliance,” and organizations should be wary of vendors claiming so.

# SEE HOW EQUINIX SMARTKEY HELPS MEET GDPR REQUIREMENTS

SmartKey creates a control layer between the data controller and the data processors to help meet GDPR requirements for data auditing, control and erasure. Specific requirements of GDPR that Equinix SmartKey helps organizations meet include:

- **Fine-grained access controls for users and data:** Only the authorized processor gets access to the required data and only for the duration for which a business case exists as required by GDPR
- **The right to be forgotten:** If a customer requests data erasure, SmartKey can delete the corresponding decryption key. Such a deletion is irreversible and is logged into the central audit log. Organizations can be assured that data cannot be used once the key has been deleted
- **Data masking:** SmartKey masks sensitive data before they are processed in a test cluster, greatly reducing GDPR compliance surface
- **Tokenization:** Customers can use SmartKey to tokenize PAN, date of birth, addresses, etc. to reduce the possibility of wrongful exposure
- **Global logging:** All accesses to personal data are automatically logged in a centrally viewable tamper-proof global audit trail. There is never any dispute about who accessed which data and when
- **Key destruction:** Once a key is destroyed, no one—not even the enterprise, Equinix or a user—can restore it. Thus, organizations can easily remove access to certain data
- **Geo-fencing:** Organizations can adopt policies based on the location of data
- **Support for multiple data processors:** Seamless support for multiple data processors in various clouds and locations makes it easy to have a compliant operation

## SmartKey has built-in features to meet GDPR requirements





## SUMMARY

GDPR is a framework for empowering customers with their privacy rights. Like any widely applicable privacy framework, organizations need to implement a complex set of measures. GDPR involves multiple groups in an organization, including security, privacy, legal, business operations, and infrastructure operations. It also creates new roles, such as the data protection officer, and possibly requires new functions, such as digitizing personal data and implementing a uniform audit trail. For this reason, there is no magic formula prescribing “use this software to achieve complete GDPR compliance,” and organizations should be wary of vendors claiming so.

Once organizations have digitized their personal data inventory and have identified appropriate access controls based on their legal needs in the form of Access Metadata, Equinix SmartKey can help them with GDPR.

SmartKey provides a uniform control plane to organizations to enforce the needed access controls. The globally available solution implements fine-grained access controls for users and data, the rights to be forgotten, pseudonymization, tokenization, a global log, key destruction, a secure audit trail, geo-fencing, and portability of keys. SmartKey, the industry's first cloud-neutral HSM as a Service, helps enterprises meet GDPR compliance, as well as offering extended capabilities to enable digital transformation when deployed on Platform Equinix®.

**GDPR requires a people, process and technology approach. Organizations will need to align their legal, operational, and business processes. Encryption and key management technologies have a fundamental role to play, and Equinix SmartKey delivers this with unparalleled simplicity.**

**Try the 30-day free trial today.**

[www.equinix.com/smartkey](http://www.equinix.com/smartkey)

This GDPR paper is derived from “Understanding GDPR beyond buzzwords and four practical steps to meet compliance” with permission from Fortanix.





EQUINIX

WHERE OPPORTUNITY CONNECTS

## Corporate HQ

Equinix, Inc.  
One Lagoon Drive  
Redwood City, CA 94065  
USA

Main: +1.650.598.6000  
Email: [info@equinix.com](mailto:info@equinix.com)

## EMEA

Equinix (EMEA) BV  
Rembrandt Tower  
Amstelplein 1  
1096 HA Amsterdam  
Netherlands

Main: +31.20.754.0305  
Email: [info@eu.equinix.com](mailto:info@eu.equinix.com)

## Asia-Pacific

Equinix Hong Kong Limited  
Units 6501-04A & 6507-08, 65/F  
International Commerce Centre  
1 Austin Road West  
Kowloon, Hong Kong

Main: +852.2970.7788  
Email: [info@ap.equinix.com](mailto:info@ap.equinix.com)

## About Equinix

---

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most-interconnected data centers. In 52 markets across five continents, Equinix is where companies come together to realize new opportunities and accelerate their business, IT and cloud strategies.

In a digital economy where enterprise business models are increasingly interdependent, interconnection is essential to success. Equinix operates the only global interconnection platform, sparking new opportunities that are only possible when companies come together.