Are You GDPR Compliant?

As the Head of Legal in Pure's Europe, Middle East and Africa region, and a qualified Data Protection Practitioner, I often engage with customers with questions about Pure's security, compliance, and data protection. I am often asked questions about Pure's data protection policies as well as how our products can be used in a GDPR compliant organization. I thought it would be helpful to share some of these discussion points via a blog on GDPR, security and encryption, one of the key benefits Pure offers to customers when considering data storage and compliance strategy for GDPR.

What Is GDPR?

The regulation applies to all organizations, regardless of location, that handle the personal data of EU residents, both digital and in other forms.

Fundamentally, GDPR declares that data subjects are the owners of the personal data that is held by others about them, and specifies both their rights surrounding it, and the obligations of entities that acquire, process and store such data with particular emphasis on keeping it secure and available. Individuals'

pers

Article 1
Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Excerpt from GDPR Article 1 defining the regulation's purpose and scope

- The right of access to it
- The right to rectify verifiable errors in it
- The right to restrict what is done with it (within certain legal limits)
- The oft-cited *right to be forgotten*—to have personal data destroyed when it no longer serves a legitimate purpose

GDPR classifies entities that deal with residents' personal data either as:

Controllers
Entities such as governments, NGOs, and businesses, whose missions require personal data handling

Processors
Entities such as document handling and information technology service providers that carry out processing tasks on controllers' behalf. A single entity can fulfill both roles, for example, a business that performs all digital data processing in-house.

Within the regulation, the term *processing* refers both to:

- Manual operations such as filing, alteration, and disclosure
- Automated processing, storage, transmission, and destruction of data in digital form.

The regulation restricts controllers and processors with regard to what personal data they may acquire and what they may do with it, and specifies requirements for protecting it against unauthorized access, loss, and destruction. Additionally, the regulation obliges processors to disclose to individuals what personal data they store and what they do with it, to rectify verifiable errors in it, and to destroy it when it is no

longer required for legitimate purposes. Finally, it outlines procedural mechanisms for compliance and lays out substantial penalties for non-compliance.

How Do Organizations Comply with GDPR?

As of May 25, 2018, entities that handle personal data of EU residents must comply with GDPR. Compliance means verifiable procedures for preventing *personal data breaches* (events that lead to "*the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."[1])

To comply with GDPR, entities need appropriate hiring, training, operating, and auditing policies, as well as robust data handling, storage, and retention policies and processes. From a digital technology standpoint, this means computing, storage, and communication facilities that, when properly managed and maintained, are high barriers to theft, unauthorized disclosure, alteration, and inadvertent and malicious destruction of personal data.

> GDPR deals primarily with policy—what personal data of EU residents may be collected, what it may be used for, how it must be protected, and what rights individuals have over it—and secondarily with technology—how data in digital form should be secured against unauthorized access, kept available for use, and destroyed when no longer needed.

GDPR deals primarily with policy—what personal data of EU residents may be collected, what it may be used for, how it must be protected, and what rights individuals have over it—and secondarily with technology—how data in digital form should be secured against unauthorized access, kept available for use, and destroyed when no longer needed.

How Can FlashArray Help?

Pure Storage makes every effort to keep data stored in its systems both *available* to authorized users and *secure* against electronic intrusion and physical misappropriation. For example:

Availability
Data in FlashArrays remains available, even when major array components fail. FlashArray immutable snapshots provide unalterable records of data sets as of key points in time.

Security
Administrators need credentials to access FlashArrays, and each has a defined role. No administrator can access or modify stored data. Arrays encrypt *all* data all the time using AES-256. Key Management

Interoperability Protocol (KMIP) servers or removable SmartCards may be added in situations where physical security is a consideration.[2]

These FlashArray features help data controllers and processors “design GDPR compliance by default” as they implement new processing systems.[3]

When combined with strong network security for “data in flight” and robust system access and data handling policies, FlashArrays can be an important component of an overall GDPR compliance strategy that protects personal data in digital form both comprehensively and cost-effectively.

When combined with strong network security for “data in flight” and robust system access and data handling policies, FlashArrays can be an important component of an overall GDPR compliance strategy that protects personal data in digital form both comprehensively and cost-effectively.

While May 25th is a key deadline for GDPR, the work doesn’t stop there. Compliance is an ongoing cycle of activities. Organizations will continue their efforts working not only on their policies but more critically paying regular attention to the processes, governance and technology that support overall compliance programs. Learn more about how Pure can help with these issues in future blogs or by visiting Pure’s Security blog.

[1] Official Journal of the European Union, 4.5.2016, Article 4(12).

[2] Pure Storage Technical Brief TB-160201, *FlashArray Data Security* describes how FlashArrays protect stored data from loss and unauthorized access, even under adverse conditions.

[3] An excerpt from GDPR Article 25 (Data protection by design and by default): “…the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”