White Paper

GDPR and Data Privacy

Matt Trudewind, NetApp
November 2018 | WP-7288

Abstract

As data privacy regulation continues to evolve, it's critical to understand how new legislation such as the General Data Protection Regulation (GDPR) can impact organizations that process personal data. Although many believe that GDPR affects only organizations located within the European Union, the fact is that many companies located outside of the European Union that processes the data of EU data subjects can potentially be impacted by the law. And the penalties for noncompliance are very high. Although it's up to each individual company to develop their own process for complying with GDPR, NetApp offers many technology solutions that simplify and support a GDPR-compliant strategy.

TABLE OF CONTENTS

LIST OF FIGURES

1 GDPR Overview

The General Data Protection Regulation (GDPR) is a European Union data privacy law that, as of May 25, 2018, replaced the existing Data Protection Directive. The primary goal of the GDPR is to protect the personal data of EU data subjects. A data subject can be defined as any individual who has their personal data collected, stored, or processed. The primary goal is addressed by a wide range of requirements for organizations that process the personal data of EU data subjects. The penalties for noncompliance with GDPR can reach the greater of €20 million or 4% of the organization's revenue. GDPR is probably only the beginning of a wave of new data privacy legislation. Therefore, it's important to develop an overall framework, based on privacy by design, for dealing with GDPR, and other privacy regulations as well.

1.1 Determining Whether Your Organization Is Affected by GDPR

At first glance, it might seem that only EU-based companies need to worry about GDPR. However, the law also applies to organizations outside of the EU that process personal data of an EU data subject in connection with goods or services offered within the EU or monitors the behavior of individuals within the EU. Organizations must determine whether they are impacted by GDPR . Where an organization is impacted by GDPR, it is very important to have a data privacy compliance strategy in place.

Examples of personal data include but are not limited to the following:

- Name
- Date of birth
- IP address
- School
- Employer
- Driver's license
- Credit score

1.2 GDPR Compliance

Currently, there is no official GDPR certification body, which means that organizations can use many different strategies, techniques, and methods to achieve compliance.

When it comes to the strict interpretation of GDPR legislation, the NetApp® product portfolio allows customers to adhere to specific portions of the legislation, but it is important to remember that technology only facilitates a company's overall compliance process.

You might assume that simply purchasing a product or solution that is marketed as "GDPR Compliant" is all that is required to avoid an audit and/or a fine. However, using the underlying technology or solution does not automatically make the organization GDPR compliant. For example, NetApp does not claim that simply buying a NetApp product or solution makes an organization GDPR compliant. This is because GDPR compliance is more about the processes and procedures for handling the personal data of EU data subjects that are in place in an organization than it is about which product or solution was used to process and store that data.

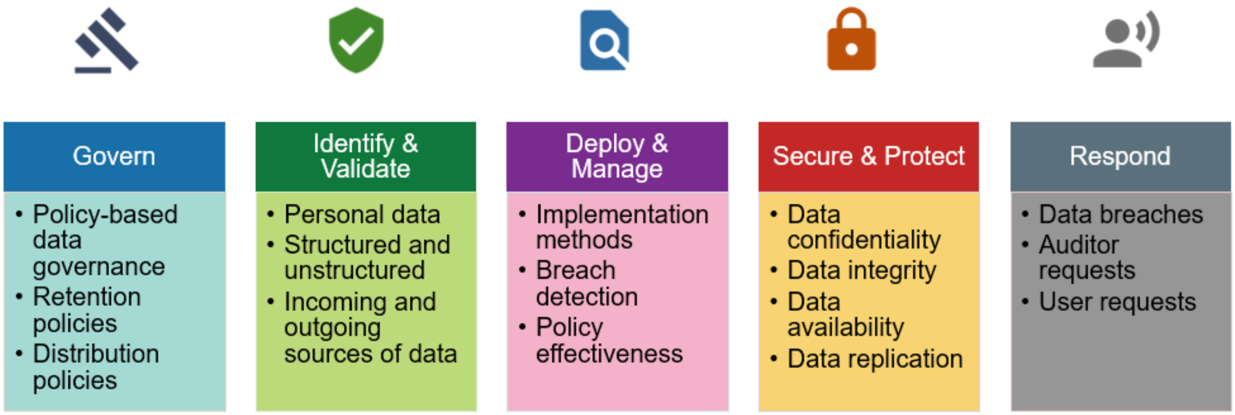
It's important to evaluate how your company collects and stores personal data. A company that does not collect or store any EU personal data might already be GDPR compliant. Once you understand how personal data is stored and collected, your goal should be to develop a data privacy framework that leverages technology to simplify the compliance process. Having a known process or framework for dealing with a privacy law like GDPR puts your company in a defensible position if a legal situation arises.

1.3 Developing a Data Privacy Framework

The goal of any organization should be to develop a repeatable and traceable process for all privacy-related issues.

A data privacy framework is essentially a customer-defined end-to-end repeatable process that describes how data privacy is handled throughout the data's life within the organization. The framework defines items like who has access to the data and where the data is stored. Figure 1 is an example of NetApp's perspective of a data privacy framework.

Figure 1) Data privacy framework example.



Govern
- Policy-based data governance
- Retention policies
- Distribution policies

Identify & Validate
- Personal data
- Structured and unstructured
- Incoming and outgoing sources of data

Deploy & Manage
- Implementation methods
- Breach detection
- Policy effectiveness

Secure & Protect
- Data confidentiality
- Data integrity
- Data availability
- Data replication

Respond
- Data breaches
- Auditor requests
- User requests

Sample data privacy framework definitions:

- **Govern.** Defines the policies and procedures of how data is to be used, controlled, and retained.
- **Identify and validate.** The process of finding the organization's data and validating that the type of data being captured is correct for the organization.
- **Deploy and manage.** Determines the organization's strategy and policies for how data is deployed and managed, including breach detection.
- **Secure and protect.** Determines the organization's methodology for making data secure, available, and protected.
- **Respond.** Defines the process of how the organization responds to a data breach, audit, or user request for data.

With this framework in place, your organization is in a better position to pass any audit that might come up and avoid any fines. Because the penalties for a violation of GDPR are quite high, it's crucial to have an internal process in place before an audit occurs.

The framework is not limited to GDPR. Once the process is defined and in place, it can be leveraged for future privacy law changes as well.

2 NetApp Technology Solutions for GDPR

This section describes how NetApp technologies can assist in working toward GDPR compliance. As mentioned earlier, however, keep in mind that technology solutions only help to enable the overall compliance process.

The NetApp solutions shown in Figure 2 do not entirely solve every item mentioned in this article. However, the solutions greatly simplify the overall development of the privacy framework.

This section discusses some of the NetApp solutions that assist in developing the three areas of the data privacy framework shown in Figure 2. Figure 3 is a graphical overview of the key NetApp technical solutions that assist with GDPR.

Figure 2) NetApp focus areas in the data privacy framework.

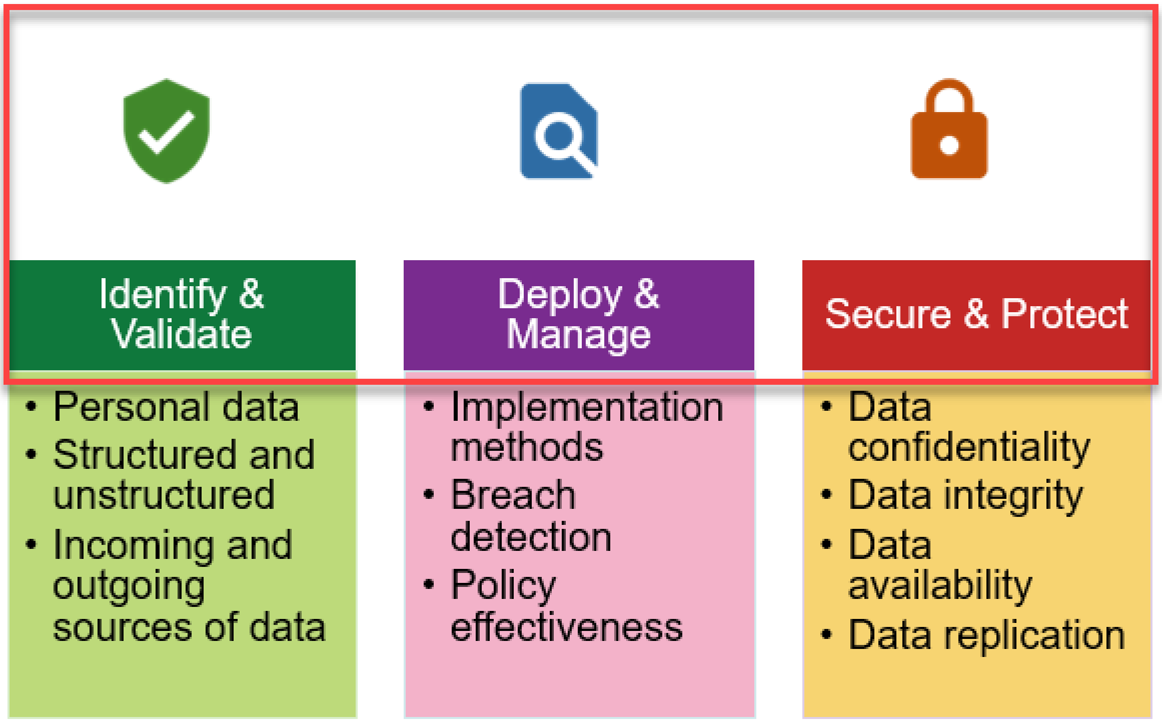
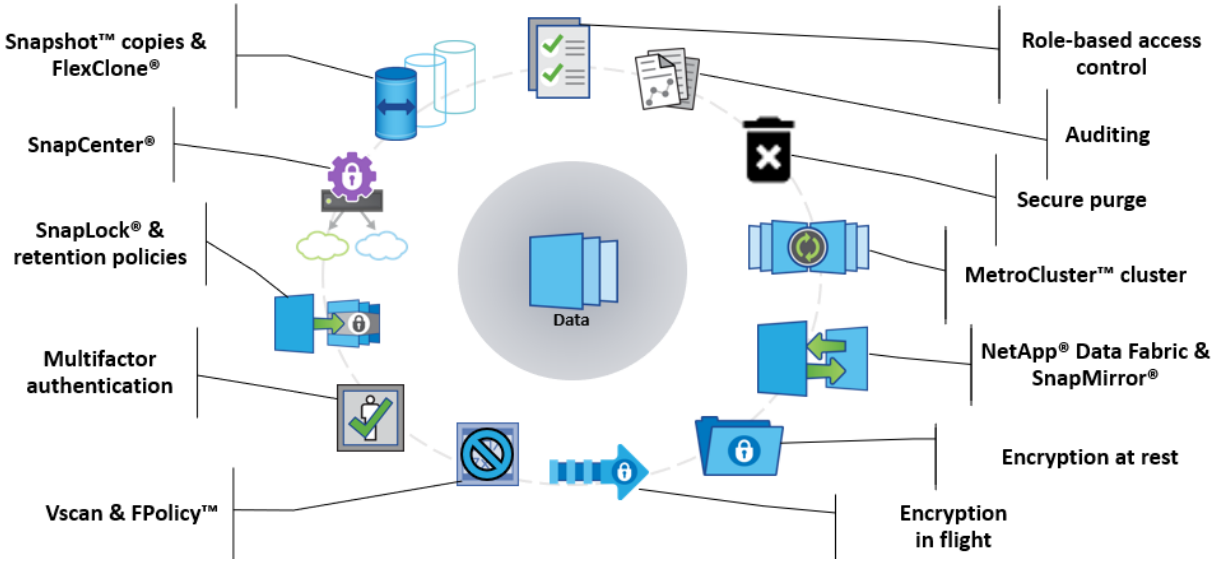


Figure 3) NetApp technology solutions that assist with GDPR.


Snapshot™ copies & FlexClone®
SnapCenter®
SnapLock® & retention policies
Multifactor authentication
Vscan & FPolicy™
Data
Role-based access control
Auditing
Secure purge
MetroCluster™ cluster
NetApp® Data Fabric & SnapMirror®
Encryption at rest
Encryption in flight

2.1 NetApp Data Fabric and SnapMirror

NetApp Data Fabric allows organizations to locate their data by using SnapMirror® based technologies where they need it, whether that is on the premises, at a third-party service provider, in the cloud, or a combination of all three. It also allows the data to be moved seamlessly within the hybrid cloud across all of these different locations by using the same underlying SnapMirror technology.

Data Privacy Framework Definition:

- Identify and validate
- Deploy and manage
- Secure and protect

Related GDPR Articles: https://gdpr-info.eu/

- Article 20: Right to Data Portability
- Article 25: Data Protection by Design and by Default
- Articles 44 – 50: Transfers of Personal Data

2.2 Snapshot Copies, FlexClone Volumes, and SnapCenter Software

NetApp ONTAP® Snapshot™ technology creates point-in-time copies of data that can be used to restore that data as needed. This capability is particularly valuable to aid in quick ransomware recovery. Snapshot copies also allow the instant creation of a separate online instance of the data by using the ONTAP FlexClone® technology. The FlexClone instance can look exactly like the original data at the time the copy was taken. Using third-party masking technology and NetApp SnapCenter®, the FlexClone data can be anonymized and processed without affecting the original data.

Related GDPR Articles: https://gdpr-info.eu/

- Article 6: Lawfulness of Processing
- Article 17: Right to Erasure (Right to Be Forgotten)

- Article 25: Data Protection by Design and by Default
- Key Issues: Privacy by Design
- Article 35: Data Protection Impact Assessment
- Articles 44 – 50: Transfers of Personal Data

2.3 SnapLock and Retention Policies

ONTAP SnapLock® compliance software uses a data retention policy to prevent any change to the data after the first write for a predetermined period of time. Once the data is written, no one can change or modify it until the SnapLock retention period has expired, providing immutable data storage.

Related GDPR Articles: https://gdpr-info.eu/

- Article 35: Data Protection Impact Assessments
- Articles 44 – 50: Data Transfers

2.4 Encryption at Rest

ONTAP can prevent data theft or loss by using encryption at rest, which makes it possible to encrypt data while it's resting by using hardware such as NetApp Storage Encryption (NSE), which encrypts the disk drives, or by using software such as NetApp Volume Encryption (NVE) to specify which volumes to encrypt. NetApp E-Series systems also provide a hardware disk encryption solution called full-disk encryption (FDE). Encryption at rest makes sure that even if an entire disk shelf is stolen, the data cannot be read.

Related GDPR Articles: https://gdpr-info.eu/

- Key Issues: Privacy by Design
- Article 32: Security of Processing
- Articles 44 – 50: Data Transfers

2.5 Encryption In Flight

ONTAP provides file-level protocol encryption for both NFS (through KRB5P) and SMB (SMB3 encryption) while the data is transmitted across the network. It supports AES-256 encryption level and ensures that the data reaches the destination without being compromised during transit.

Related GDPR Articles: https://gdpr-info.eu/

- Key Issues: Privacy by Design
- Article 32: Security of Processing
- Articles 44 – 50: Data Transfers

2.6 RBAC

Role-based access control (RBAC) allows administrative accounts to be restricted and/or limited in what actions they can take on the system. Both ONTAP and E-Series systems support this capability, which prevents a single account from being allowed to perform all potential actions available on the system.

Related GDPR Articles: https://gdpr-info.eu/

- Key Issues: Privacy by Design
- Article 32: Security of Processing

2.7 Multifactor Authentication

Multifactor authentication (MFA) can be configured to mandate authentication of system administration accounts through a verified third-party identity provider. This process helps to verify that an actual administrator is the one using the admin account.

Related GDPR Articles: https://gdpr-info.eu/

- Key Issues: Privacy by Design
- Article 32: Security of Processing

2.8 Auditing

ONTAP and E-Series both have verbose audit logging capabilities by default, which provides a full record of what has occurred on the system in case of an audit.

Related GDPR Articles: https://gdpr-info.eu/

- Article 7: Conditions for Consent
- Article 15: Right of Access
- Article 16: Right to Rectification
- Article 17: Right to Erasure (Right to Be Forgotten)
- Article 18: Right to Restriction of Processing
- Article 20: Right to Data Portability
- Article 21: Right to Object
- Article 33: Notification of a Personal Data Breach to the Supervisory Authority
- Article 34: Communication of a Personal Data Breach to the Data Subject
- Article 35: Data Protection Impact Assessment

2.9 Vscan and FPolicy

ONTAP Vscan and FPolicy™ are aimed at malware prevention. Vscan provides a way for NetApp antivirus scanner partners to verify that files are virus free. FPolicy integrates with NetApp partners to monitor file access behaviors and to prevent unwanted access or change to files based on policy settings. This helps prevent ransomware from getting a foothold in the first place.

Related GDPR Articles: https://gdpr-info.eu/

- Article 7: Conditions for Consent
- Article 15: Right of Access
- Article 16: Right to Rectification
- Article 17: Right to Erasure (Right to Be Forgotten)
- Article 18: Right to Restriction of Processing
- Article 20: Right to Data Portability
- Article 21: Right to Object
- Article 33: Notification of a Personal Data Breach to the Supervisory Authority
- Article 34: Communication of a Personal Data Breach to the Data Subject
- Article 35: Data Protection Impact Assessment

2.10 Metro Cluster Cluster

A NetApp MetroCluster™ cluster is a zero-recovery point objective (RPO) ONTAP solution that provides data availability across large distances, typically for business continuity across different campuses.

Related GDPR Articles: https://gdpr-info.eu/

- Article 20: Right to Data Portability
- Article 25: Data Protection by Design and by Default
- Articles 44 – 50: Data Transfers

2.11 Secure Purge

In ONTAP 9.4 and later, secure purge provides the capability to cryptographically shred individual files from solid-state drives (SSDs) with no down time. All other files remain untouched and online. This is important because when you delete a file from an SSD drive it doesn't necessarily overwrite or remove that file due to flash drive wear leveling. GDPR requires "right to erasure," and secure purge is a key feature that addresses that requirement for SSDs.

Related GDPR Articles: https://gdpr-info.eu/

- Article 17: Right to Erasure (Right to Be Forgotten)

3 Summary

Data privacy laws and regulations continue to require organizations to protect individuals' personal data, no matter where that data may live. GDPR is probably only the first of many such changes to come. Another recent piece of legislation in the privacy arena is the California Consumer Privacy Act of 2018. NetApp offers a comprehensive set of technology solutions that can help organizations meet their data privacy framework goals.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NetApp GDPR Site
  www.netapp.com/us/info/gdpr.aspx
- NetApp Data Security Site
  www.netapp.com/us/products/data-security/index.aspx
- NetApp Partner Directory
  https://partner-connect.netapp.com/us/partner-directory
- FPolicy Solutions
  www.netapp.com/us/search/index.aspx?q=fpolicy

Version History

Version	Date	Document Version History
Version 1.0	October 2018	Initial Release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Trademark Information