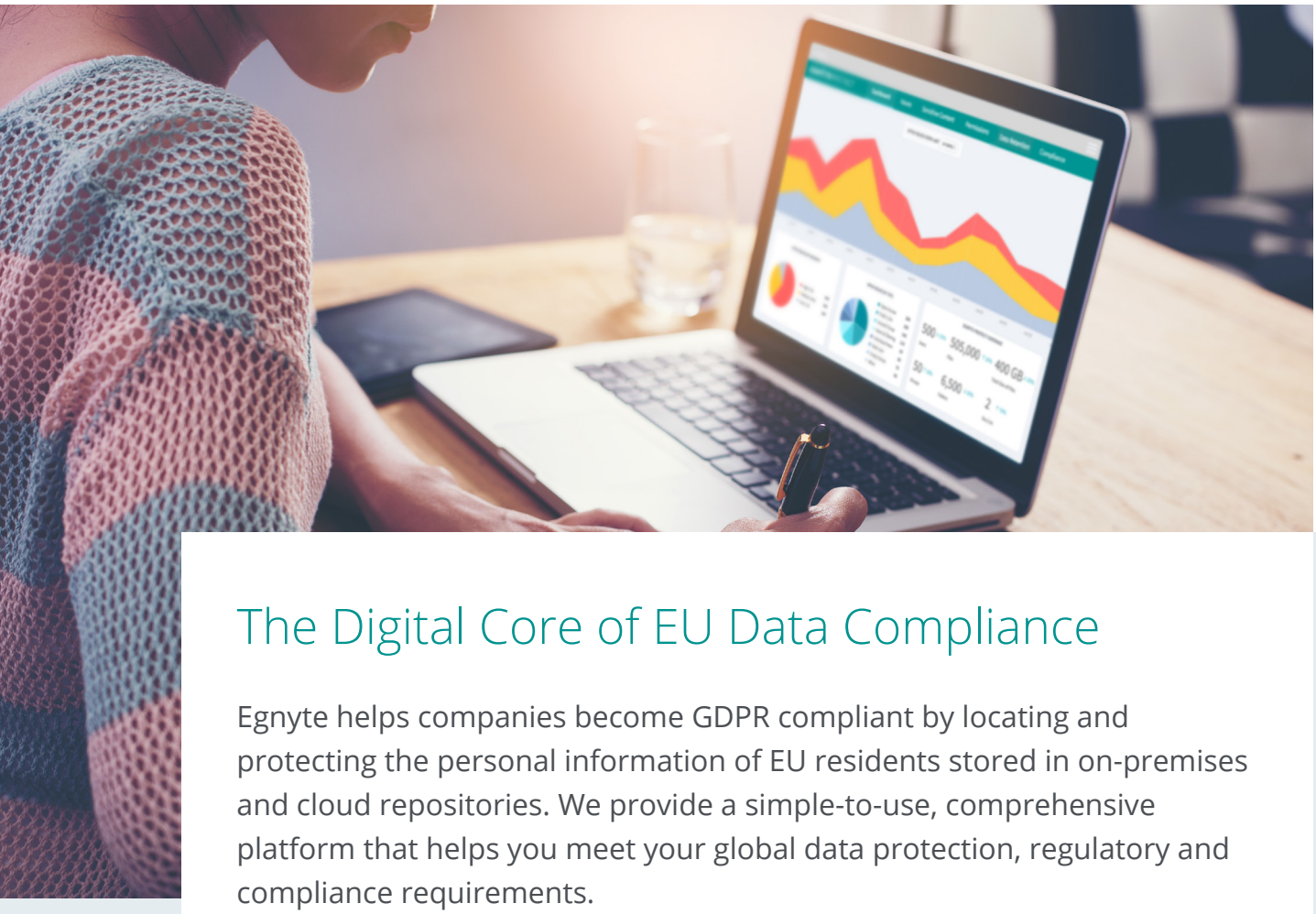
EGNYTE

# How Egnyte Addresses Key GDPR Requirements



## The Digital Core of EU Data Compliance

Egnyte helps companies become GDPR compliant by locating and protecting the personal information of EU residents stored in on-premises and cloud repositories. We provide a simple-to-use, comprehensive platform that helps you meet your global data protection, regulatory and compliance requirements.

# How to approach the GDPR

Focus on the following to meet the digital requirements of the GDPR:

## Data classification

Know where personal content is stored in your cloud and on-premises repositories (specifically in unstructured data). It is critical to be able to scan the file content and identify the sensitive information in order to decrease the overall footprint.

## Access control

Know who has access to what data, know who should be authorized to access that data, and limit permissions based on employee roles (e.g. role-based access controls).

## Subject access rights

Data subjects can request confirmation of whether or not their personal content is being stored. When that is the case, they also can request to be provided access to the personal content.

## Breach notification

Under the GDPR, IT security teams should have a method/ tool to provide continuous monitoring. The tool should be able to identify unusual access patterns for files containing personal content and be able to immediately report any abnormal behavior.

With the GDPR in effect, global organizations will have to make changes in how they handle personal content.

It is critical to choose a content management platform that helps you meet the major GDPR requirements.

# Below we've defined some of the major GDPR requirements and how Egnyte helps you to address them

## Article 17: Right to Erasure (Right to be forgotten)

**What it means**

Data subjects can request that their personal content be found and deleted.

**How Egnyte addresses it***

Egnyte puts you in control of the content stored in your cloud and on-premises repositories. You can scan all Egnyte supported repositories to locate and identify personal content, classify the data, and determine what personal content belongs to an individual. You can then delete the content as required.

You can also set retention schedules and security policies for content moved to the trash.

## Article 15: Right of access by the data subject

**What it means**

Data subjects can obtain from the data controller confirmation of whether or not their personal content is being processed, and when that is the case, be provided access to their personal content.

**How Egnyte addresses it**

Egnyte enables you to access and export the personal content stored in a cloud and on-premises repositories that Egnyte supports. You must define your own subject access request policies and procedures, but Egnyte has comprehensive subject access request capability which includes content classification, notification, right to be forgotten, and data portability.

Subject access request workflow that can be used to access and export the data subject's personal content:

- You can search for an individual's personal content stored in Egnyte-supported cloud and on-premises repositories
- Details about the individual's personal content can be exported in a simple readable document format
- Files with such personal content can be downloaded by the data subject after redaction of all other sensitive information

## Article 20: Right to data portability

**What it means**

Data subjects can request the personal content provided to the data controller be returned in a structured, commonly used and machine-readable format that can be shared with other controllers.

**How Egnyte addresses it**

Egnyte enables you to process subject access requests, including the right to be forgotten and data portability.

## Article 25: Data Protection by Design and By Default

**What it means**

Embrace accountability and privacy by design as a business culture.

Implement appropriate technical and organisational measures, in an effective manner and integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

**How Egnyte addresses it**

Egnyte delivers a content management platform that enables you to monitor and control your data.

While you are responsible for limiting the collection of personal information in your business processes, Egnyte allows you to set, monitor and fix access controls to ensure least privileged access, protecting the rights of data subjects. Egnyte also provides tools like whitelisting and remediation to shrink the footprint of sensitive content.

## Article 30: Records of processing activities

**What it means**

Implement organizational and technical measures to properly process personal content.

**How Egnyte addresses it**

Egnyte enables you to classify data to create an asset register of sensitive files. Access control features let you see who has access to what data, and know who is accessing it. With data retention policies you are able to set when data can and should be deleted.

Egnyte also provides tools like whitelisting and remediation to shrink the footprint of unpermitted sensitive content.

## Article 32: Security of Processing

**What it means**

Implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal content.

**How Egnyte addresses it**

GDPR requires that you implement measures to ensure the security and confidentiality of personal content.

All files within Egnyte are encrypted at access, in transit and at rest using AES 256-bit

encryption. You are responsible for ensuring Egnyte encryption meets your security requirements.

Egnyte can provide an audit report showing the actions taken by customers to set up classification policies, issue and sensitive content remediation, and more.

Egnyte delivers an added level of security and privacy with Egnyte Key Management. Two options for key management are offered: Egnyte can manage the keys (default) or you can manage the keys (BYOK approach).

## Article 33: Notification of personal data breach to the supervisory authority

**What it means**

Notify supervisory authorities of data breach activity within 72 hours of discovery.

**How Egnyte addresses it**

Egnyte detects unusual activity (e.g. excessive file downloads) compromised accounts and potential external exposure points which could lead to a data breach. Automatic, real-time alerts can immediately notify the appropriate personnel so that they can determine if a breach has occurred, as well as take action to stop it.

If a data breach occurs, Egnyte lets you create and send a data breach report within 72 hours after it occurs. The report contains the list of data subjects impacted by the breach, along with the details of the sensitive information involved in the breach.

## Article 34: Communication of personal data breach to the data subject

**What it means**

If a data breach occurs that puts the rights and freedoms of a data subjects at risk, you must inform them.

**How Egnyte addresses it**

When a data breach occurs, Egnyte enables customers to provide details of the breach including a report containing a:

- List of the impacted data subjects with contact details
- Details about the sensitive information found in the breach

# Egnyte helps organizations of all sizes meet digital requirements of the GDPR.

We help  simplify much of the complexity behind GDPR compliance.

EGNYTE

See how Egnyte addresses GDPR

REQUEST DEMO

*These major GDPR requirements are a subset of the GDPR, and are not intended as legal advice. In order to achieve complete GDPR compliance, your internal teams should review and address all GDPR requirements.