egress

A three-step approach to help meet **EU GDPR compliance**

Helping customers protect data and manage risk in order to **prevent breaches and comply with European legislation**.

The legislation requires every business that handles EU citizens' data to maintain the privacy and security of that data, as well as manage the risks associated with handling this information. To ensure compliance, organizations will need to have systems and processes in place to protect the unstructured data contained in files, folders and emails that they control and share.

A three-step approach to compliance

1. Data audit

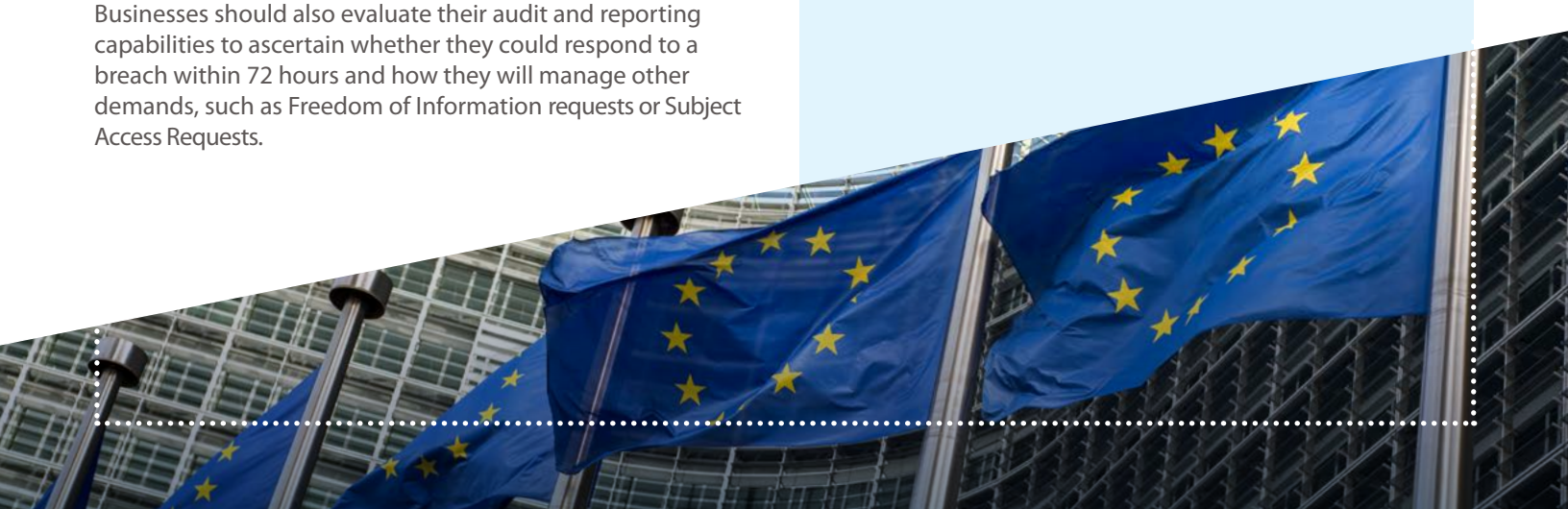
Before any organization invests in new systems and/or procedures, they need to understand how they store and handle personal data. If data is stored internally, are processes in place to effectively manage and protect it? If data is stored externally, has the supply chain been audited to understand where the data resides? Organizations also need to consider the security certifications of their hosting providers, as well as contractual terms and service level agreements.

2. Control and reporting

Often, data is most vulnerable at the point it is shared. This could be the result of an email being sent to the wrong recipient or data being shared via a third party collaboration website. The GDPR will require organizations to be able to demonstrate they have put in place the necessary technology and training to protect shared information. This should include policies that can automatically apply encryption, so that regardless of a breach, the underlying data remains secured. Businesses should also evaluate their audit and reporting capabilities to ascertain whether they could respond to a breach within 72 hours and how they will manage other demands, such as Freedom of Information requests or Subject Access Requests.

The key facts

- **What are the rules on breach notifications?**
  Under the new law, all businesses will be mandated to notify the national regulator of a data breach within 72 hours, when an individual's rights and freedoms have been compromised.
- **What will businesses have to report on?**
  Businesses will be required to explain in detail the cause, scale and anticipated impact of the breach. They will also need to demonstrate adequate investment in the protection of personal data through process, procedure and technology.
- **What are the potential fines for a breach?**
  If an organization is found to have failed in its duty to protect personal data, anticipated fines could be as much as 4% of annual turnover or $25m, whichever is higher. Data subjects are also entitled to bring their own legal action against an organization, with no cap to the potential fines.



"Under the new law, all businesses will be mandated to notify the national regulator of a data breach within 72 hours"

"Fines could be as much as 4% of annual turnover or €20m, whichever is higher"

3. A future-proofed approach

Technology decisions made today need to consider potential changes in the future. Chosen technology providers need to demonstrate a high degree of product flexibility. With the majority of businesses expected to transition to Microsoft Office 365 or similar cloud-based platforms in the next two to five years, can the chosen provider offer the required levels of integration, assurance and security in the cloud? Also, do they have the necessary independent security certifications, such as ISO 27001?

How can Egress help?

- **Data management**
  Egress offers a range of data hosting options including on-premise, hybrid or in the cloud, with providers such as Microsoft Azure and Amazon Web Services.
- **A platform approach**
  The Egress platform enables customers to protect and control data throughout its lifecycle. From email classification, to email and file encryption, secure online collaboration, secure archiving and compliance reporting.
- **Complete control**
  Egress enables users to stay in control of shared information using comprehensive audit logs, message restrictions and revocation so only intended recipients can access shared data.
- **Compliance audit and reporting**
  Egress offers the ability to index, archive and instantly search plaintext and encrypted email and file content. Organizations can then understand and analyze their data, in order to quickly perform internal investigations in response to heightened compliance requirements.
- **Securing Office 365**
  Egress is the go-to security partner for Office 365, bringing integrated email encryption, auditing and reporting to hosted environments.
- **Preventing the accidental send**
  Egress can prevent accidental data breaches by warning users about incorrect recipients before they send sensitive emails and files.

About Egress

Egress takes a people-centric approach to data security – helping users receive, manage and share sensitive data securely to meet compliance requirements and drive business productivity. Using machine learning, Egress ensures information is protected relative to the risk of a data breach and reduces user friction to ensure smooth adoption.

info@egress.com
1-800-732-0746
@EgressSoftware
www.egress.com