Egress and **EU GDPR compliance**

Achieving **technical compliance with the GDPR** using Egress data privacy and risk management solutions.

The EU General Data Protection Regulation (GDPR) has far-reaching impact for organisations operating in member states, as well as those located elsewhere that process EU citizens' data. The Egress data privacy and risk management platform can be used to comply with articles of the GDPR that specify personal data must be made technically secure, as well as aiding subject access requests (SARs), the right to be forgotten, security and restriction of processing, rectification and erasure of personal data, and notifying regulatory authorities and data subjects about breaches.

Understand, monitor and report

Egress eDiscovery and Analytics

Providing indexing, archiving and instant search of plaintext and Egress encrypted email content, Egress eDiscovery and Analytics enables organisations to **understand and analyse** their data for GDPR compliance reports and investigations.

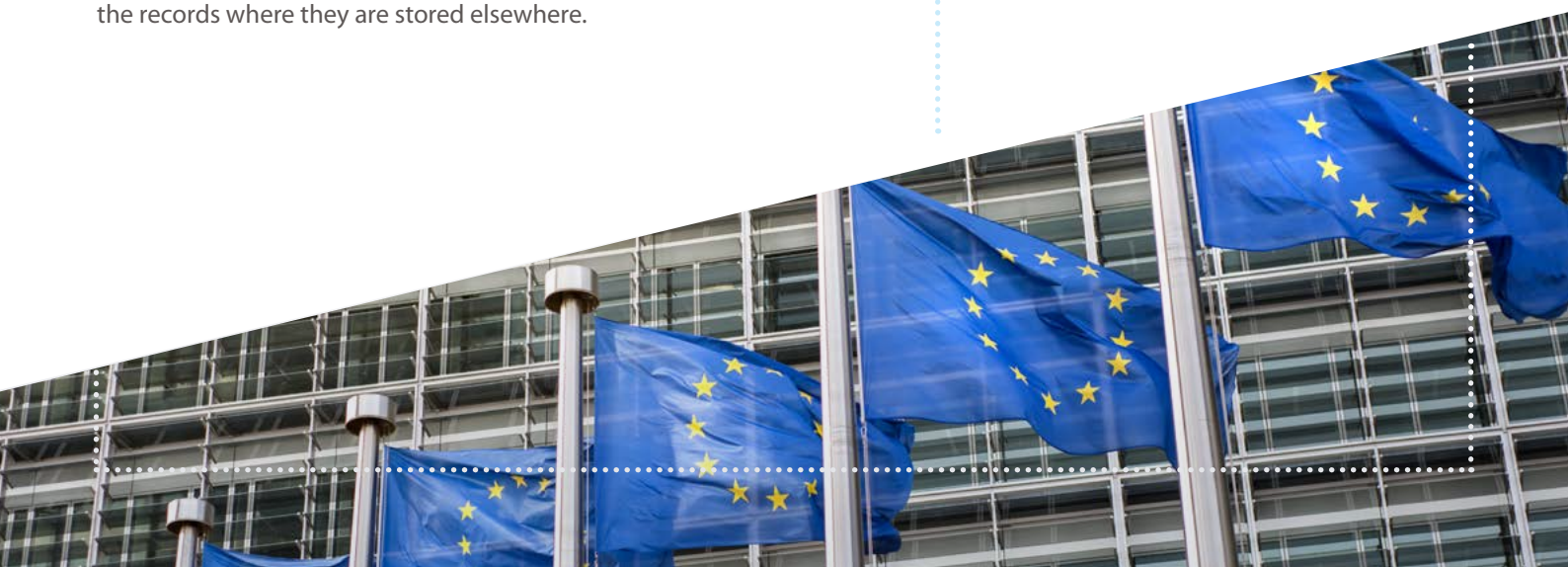
eDiscovery and Analytics takes a forensic and tamper-proof copy of all emails sent and received, providing a single view of whether personal data has been shared via email with processors and third parties. This includes when the email was sent, how many recipients it was sent to and who they are, what was contained within the email and any attachments, and whether it was sent encrypted or in plaintext. Should an email breach need to be reported, this can enable controllers to understand how many subjects / records were affected and the risk of unauthorised access to the data.

DLP reports aid GDPR compliance by highlighting emails sent both internally and externally that contain personal data but don't have the right levels of security applied to protect it. This can be used to provide ongoing improvement to the organisational and technical measures in place to secure personal data.

The **SAR report** template can be easily configured to include a subject's identifiers and then used to search all email data, associated files and related connectors. This report can be used to compile a SAR response or fulfil erasure and restriction of processing requests. Where data needs to be erased, eDiscovery and Analytics offers 'delete all' functionality for records stored within the archive and can prompt administrators to delete the records where they are stored elsewhere.

Related GDPR articles

- 15 Right of access by the data subject
- 17 Right to erasure
- 18 Right to restriction of processing
- 19 Notification obligation regarding the rectification or erasure of personal data or restriction of processing
- 32 Security of processing
- 33 Notification of a personal data breach to a supervisory authority
- 34 Communication of a personal data breach to the data subject



Identify and manage personal data

Egress Email Classification

Egress Email Classification adds visual and system identifiers to personal data, **mandating how it is handled** by internal staff, processors and third parties. To improve security, document classification can be automated via integrated DLP policies for GDPR compliance. Additionally, classification can be used to **force encryption of personal data** when it is being shared using Egress Secure Email and File Transfer or, in some circumstances, prevent release altogether.

Prevent email data breaches

Egress Risk-based Protection

Analysing users' sharing trends and historic interactions, Egress Risk-based Protection alerts staff when they are about to send information to the wrong people. This can **prevent the release of personal data to unauthorised recipients** before it happens, ultimately preventing a data breach. Users can also be alerted when recipients have been added to the 'To' or 'Cc' fields, rather than the 'Bcc' field, when sending a mass email.

Additionally, the system can notify central administrators of unusual sharing patterns and when a user chooses to override warnings about incorrect recipients.

Related GDPR articles

- 15 Right of access by the data subject
- 17 Right to erasure
- 18 Right to restriction of processing
- 19 Notification obligation regarding the rectification or erasure of personal data or restriction of processing
- 32 Security of processing
- 33 Notification of a personal data breach to a supervisory authority
- 34 Communication of a personal data breach to the data

Encrypt and control personal data

Egress Secure Email and File Transfer

Egress Secure Email and File Transfer provides government and industry-certified security and authentication for protecting email contents and attachments, including large files, in transit and at rest. The solution integrates with Microsoft Outlook, Office 365 and G Suite for easy-to-use one-click encryption and supports multi-factor authentication, customisable policy control and access to secure information via mobile devices.

Detailed audit logs enable users to track information even after it has been shared, with the ability to revoke access in real time should recipients no longer be authorised to access information. Additionally, policy control can prevent actions such as downloading data locally, copy and pasting information, and using print screen functionality. When implemented at the gateway, outgoing emails can be **encrypted based on key terms** for GDPR compliance.

End-to-end security is ensured by recipients being able to reply and initiate secure emails and file transfers to Egress subscribers for free.

Encrypted collaboration environment

Egress Secure Workspace

Egress Secure Workspace is an encrypted environment for sharing and storing files, editing documents, and annotating PDFs in real time. Access to and handling of personal data can be controlled using multi-factor authentication and comprehensive user permissions, including preventing local downloads of files and restricting editing.

Detailed audit logs enable users to **track information after it has been uploaded** into Secure Workspace, with the ability to revoke access in real-time should recipients no longer be authorised to access information.

End-to-end security is ensured as authorised third party recipients are able to access Secure Workspace free of charge.

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
0844 800 0172
@EgressSoftware
www.egress.com