Egress and EU GDPR compliance

Achieving **technical compliance with GDPR** using Egress Human Layer Security solutions.

The General Data Protection Regulation (GDPR) has transformed the legal frameworks that govern the use of personal data for EU citizens - with non-compliance opening the door to financial penalties, damaged reputations and costly litigation. Our Human Layer Security solutions allow your business to effectively comply with GDPR as employees share confidential data via email and file transfer, and respond to Subject Access Requests (SARs).

Fast-tracking analytics and reporting for GDPR

Egress Investigate

With indexing, archiving and instant search of both plaintext and Egress-encrypted email content, we help you to measure the risk of a breach and quickly analyse data for GDPR compliance reports and investigations.

We take a forensic and tamper-proof copy of all outbound and inbound emails, and can instantly provide you with a comprehensive view of sensitive email data flows (including when an email was sent, the number and identity of recipients, email content and attachments, and the level of encryption applied and when encrypted content was accessed by recipients).

We also help you to accelerate responses to SARs from citizens with an easily configurable template that uses elastic search technology to search all email data and associated files within seconds, giving you critical time back to deploy resources elsewhere in the business. You can then use our automated redaction tools to remove non-pertinent sensitive data, so you can remain compliant with GDPR throughout the SAR process.

Relevant 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

Stop email data breaches

Egress Prevent

We use contextual machine learning to analyse and continously learn user behaviour so that we can spot abnormal actions and stop security breaches before they happen.

We interrogate email recipients and domains, subject line, and message body and attachment content to make sure that the right data is going to the right recipient(s). Our unobtruive plug-in makes life easy for users to prevent errors, while our mobile app means that your employees can prevent mistakes on the go.

"Without Egress, we would have had to buy at least five different systems to meet our information sharing requirements."

HEAD OF INFORMATION GOVERNANCE AND SECURITY, HCA HEALTHCARE

Secure the file sharing process

Egress Secure Workspace

Our file sharing and collaboration platform provides industry and Government and industry-certified security for sharing and storing files, editing documents in real time, and annotating PDFs. Administrators can control access to, and handling of, personal data using multi-factor authentication and comprehensive user permissions.

Detailed audit logs also allow you to track information after it has been uploaded into Secure Workspace, and you can fully revoke access to files in real time if a recipient is no longer authorised to access content.

Approproriately secure sensitive data

Egress Protect

We provide Government and industry-certified security and authentication to encrypt email content and attachments, including large files, in transit and at rest.

We've simplified the sender experience using contextual machine learning to dynamically automate security. Our solution also integrates with Microsoft Office 365 and Outlook for a streamlined user experience, and our mobile apps support working on the go.

Our contextual machine learning also improves the recipient experience, making end-to-end email security easier by removing the risk of user avoidance. Egress Smart Authentication continuously learns from individual recipient's domains and locations, building trust to seamlessly authenticate access to Egress-encrypted emails.

In addition, we provide comprehensive audit logs for real-time monitoring and compliance purposes. Our email recall can be used when recipients are no longer authorised to view sensitive content, and our enterprise-grade policy controls mean you can prevent potentially damaging actions, such as data downloads, copy / pasting, and usinf print screen functionality. We also provide multi-factor authentication when you require further assurance over recipient identities.

For more information please contact your account manager or call 0844 800 0172

About Egress

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we provide human layer security to protect individual users and stop breaches before they happen.

www.egress.com | info@egress.com | 0844 800 0172 | @EgressSoftware