Data Privacy **the Egress approach**

As a data security business, data privacy forms a core part of the Egress Software Technologies Group's ethos and services – both in their design and delivery. Egress takes its obligations very seriously and recognises the importance of compliance both within its own business and those of its customers.

How does Egress document its compliance with data laws?

Egress has extensive internal policy documentation in place which describes its approach to its obligations under the data protection laws relevant to the jurisdictions in which it operates. These ensure that it is focussed on compliance by embedding data privacy and security behaviours within its day-to-day activities.

Egress also provides information to customers and users about its services to enable them to not only understand how the services are delivered to them, but also to provide them with the information they need to ensure that they are themselves able to meet their own obligations in respect of data privacy and transparency.

Egress understands that its customers and users trust it with the data that they upload, send and share using its services (what Egress refers to as "Content"). That is why it wants to make sure that they understand how this is protected.

How does Egress protect data?

Egress treats the data that it collects, stores and processes in providing its services as falling into 4 categories:

Type of Data	Definition	How does Egress help to protect it?
Content	the files, data, text, audio, video, images and other materials that are transferred, stored, shared or hosted on or through the services, software or support by customers, users and recipients, including any personal data in it. It does not include CRM Information, Smart Data or System Data.	A high level overview of the measures Egress takes to protect the personal data in the Content can be found at www.egress.com/legal/technical-measures.
CRM information	the databases, logs and other collections of personal data about customers and users that is provided to Egress by customers, users, or that Egress obtains in connection with: (i) the creation and administration of accounts; (ii) how the services, software and support are used, accessed and interacted with; (iii) any	Egress has a Supplier On-boarding process in place to ensure that appropriate compliance and regulatory checks are carried out and information received. The Egress Information Security team conduct audits on its suppliers

Type of Data	Definition	How does Egress help to protect it?
	permissions, consents or preferences; and (iv) entities or individuals being Egress customers, and information that Egress obtain from third parties that may be linked to them or their organisation.	appropriate to the services that they provide.
Smart Data	the record of individual user email behaviour and associations formed from the machine learning and artificial intelligence led processing, collection and analysis of email metadata (e.g. date and time, sender and recipient email addresses, package classification and other unique and non-unique message identifiers) and other domain, location and 'trust' data. This excludes CRM Information and System Data.	Smart Data is stored in infrastructure provided by Egress' Cloud Hosting Supplier. Access to Smart Data is restricted with access controls including Multi-Factor Access (MFA) and perimeter network controls; aligned with our ISO27001 certificate and cloud security principles. All production environments undergo regular vulnerability scanning.
System Data	(i) usage statistics, system logs, performance and security data, feedback data, records of support requests, and aggregated data about how Egress sites, services, software, support and apps are used (e.g. performance counters, access logs, metrics and associated metadata, unique identifiers for devices, technical information about the devices used, the network, operating system and browsers); and (ii) data identified as malicious (e.g. malware infections, cyberattacks, unsuccessful security incidents, or other threats). This may contain limited CRM Information where it appears, for example, in log records but excludes Smart Data.	System Data is stored in infrastructure provided by Egress' Cloud Hosting Supplier. Access to System Data is restricted with access controls including Multi-Factor Access (MFA) and perimeter network controls; aligned with our ISO27001 certificate and cloud security principles. All production environments undergo regular vulnerability scanning.

What certifications and standards does Egress adhere to?

Egress is ISO:27001 certified and assessed annually to ensure that it continues to adhere to this well recognised and respected standard.

Egress Software Technologies, Inc. has certified its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks to the U.S. Department of Commerce and has been added to the Department's List of self-certified Privacy Shield participants.

Further details about Egress' certifications can be found at www.egress.com/certifications.

Is Egress an owner/Controller or provider/Processor of personal data/PII?

The companies within the Egress group perform both of these roles depending on the nature of the personal data/PII in question.

Type of Data	Egress Group company's role
Content	Provider/Processor or sub-Processor
CRM information	Owner/Controller
Smart Data	Owner/Controller
System Data	Owner/Controller*

Customers may themselves be an independent Owner/Controller, not a joint Owner/Controller with Egress, of certain information within these data sets

* Egress is, in certain circumstances, an Owner/Controller. For example, this may include when Egress (a) carries out forensic investigations into potential or actual security breaches, including in the case of a personal data/PII breach, and unsuccessful security incidents; (b) carry out system, service and software development and servicing in accordance with its privacy policies; and (c) carry out security reviews of our systems, networks, software and services (both on a holistic and on a customer specific level), and including when Egress may commission third-parties to carry out security testing, including penetration and vulnerability testing.

Where can I find key information about data privacy at Egress?

There is a large range of data privacy resources available at www.egress.com/legal including:

Platform and service privacy policy	www.egress.com/privacy-policy	describes how data is collected, stored and processed when using Egress services
Website privacy policy	www.egress.com/website-privacy	describes how data is collected, stored and processed when using Egress' website and apps
Visitor privacy policy	www.egress.com/legal/visitor-privacy	describes the data collected, stored and processed when visiting Egress premises
Event privacy policy	www.egress.com/legal/event-privacy	describes the data Egress collects, stores and processes when an individual speaks to Egress and its representatives at an event
Recruitment privacy policy	www.egress.com/legal/recruitment-privacy	describes how data is collected, stored and processed when an individual applies for a role with the Egress group
Individual rights	www.egress.com/legal/your-rights	sets out the rights that individuals have by law and how they can exercise them in

		respect of personal data/information that Egress is the owner/Controller of
Sub-processors	www.egress.com/subcontractors	sets out third-parties involved in the delivery of Egress' services
Third Party Disclosure Requests	www.egress.com/legal	describes Egress' approach when it receives a disclosure request from a third-party (such as a law enforcement agency)
Deletion and Retention	www.egress.com/legal	outlines the retention policy applicable to the different types of data collected, stored and processed by Egress
Technical measures	www.egress.com/legal/technical-measures	provides a summary of the technical measures that Egress takes to protect Content and its networks.
Certifications	www.egress.com/certifications	details the third-party certifications and standards that Egress complies with and adheres to
Products	www.egress.com/solutions-menu www.egress.com/datasheets	information about Egress' products, the security they offer and how they can help customers and users to meet their own data privacy and security obligations

Does Egress use sub-processors and sub-contractors?

Yes. As is common with many Software-as-a-Service businesses, Egress uses certain specialist sub-processors (e.g. datacentre providers, support platform software providers), and other Egress group companies, in the delivery of its services. Non-Egress third-parties are subject to terms that comply with relevant data privacy legislation and ensure that any processing that they carry out is only for the purposes of providing their specialist services to Egress and its customers/users. They do not have any rights to use any personal data/PII for their own purposes.

You can find out more information about them on Egress' website at www.egress.com/subcontractors where you can also sign up to receive email alerts if Egress makes changes to the sub-processors it uses.

How is data deleted and retained?

Egress' data retention policy is available at www.egress.com/legal.

How are data subject rights respected?

Egress recognises that individuals across the globe may have certain rights provided with by law. Details on how Egress itself enables individuals to exercise these rights is set out at www.egress.com/legal/your-rights. Egress provides assistance to its customers in line with its legal obligations and passes on any relevant request to a customer that relates to personal data that Egress is not the Owner or Controller of.

Please remember, if data subjects/individuals seek to exercise rights in relation to personal data that forms part of your Content, Egress will pass these requests to you in your role as Owner/Controller of that personal data/PII.

Egress may also direct the data subject/individual to contact you directly in relation to their request. Egress may provide your basic contact information to enable them to do this.

The customer or user will need to respond to/action them appropriately and in accordance with relevant legal timescales.

Does Egress disclose data to third-parties?

Third-parties may be involved in the delivery of the services (see the section on Sub-processors and sub-contractors above).

Egress only discloses data where it is required to do so to respond to a lawful request. You can find out more about Egress' approach to these requests at www.egress.com/legal.

Does Egress have a Data Processing Addendum?

Yes. It can be found at www.egress.com/legal. If you took out or renewed your subscription between April 2018 and June 2019 you do not need to sign this document.

Has Egress self-certified with the EU-U.S. Privacy Shield?

Yes. Egress Software Technologies, Inc. has certified its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks to the U.S. Department of Commerce and has been added to the Department's List of self-certified Privacy Shield participants.

In order to achieve this approval, the Egress Software Technologies Group's data privacy documentation, policies and procedures were externally reviewed for their compliance with these frameworks which closely align to the requirements of the General Data Protection Regulation.