Data Retention Policy

Customer Platform and Services

Version 1.06 (24 January 2019)

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

Policy **definitions**

The following terms are used in this Policy:

Account Information	the databases, logs and other collections of Personal Data about a Customer and its Users that is provided to us by the Customer, its Users, or that we obtain in connection with: (i) the creation and administration of its and their accounts; (ii) its and their use of the Platform, Software and Services (e.g. how they're used, accessed and interacted with); (iii) any permissions, consents or preferences that are given to us; and (iv) it being Our customer, and information that we obtain from third parties that may be linked to the Customer.
Content	the files, data, text, audio, video and images that are transferred, stored, shared or hosted on or through the Platform, Software or Support by you, Users and third parties, including any Personal Data in it. It does not include Account Information, Threat Protection Data or System Data.
Customer	an individual, company, organisation or other entity that has entered into an agreement with: (i) a Group company (whether directly or through an approved reseller); or (ii) one of the Group's approved managed service providers, in each case under which it (and where relevant, its group companies and Users) are granted access to, and use of, the Platform and requested Services. Any managed service provider must have its own contractual relationship with the relevant Group company
Group	Egress Software Technologies Limited (company number: 06393958, registered office: 12th Floor, White Collar Factory, 1 Old Street Yard, London, EC1Y 8AF, United Kingdom) together with its holding company, or any subsidiary of it or its holding company, or any other company under common control with it from time to time.
Personal Data	any information relating to an identified or identifiable natural person (**data subject**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Platform	the Group's proprietary 'software-as-a-service' solution and associated functionality and services.
Platform Software	that part of the Platform's software necessary to enable a Customer to install the Platform onto its own infrastructure where it's purchased an on-premise or hybrid solution.
Plug-Ins	one or more proprietary or third party software components or plug-ins provided by our Group for installation on a Customer's infrastructure.
Services	professional services and support that the Group companies provide to Customers in accordance with the terms of the relevant agreement in place with the Customer.
Software	collectively Plug-Ins and Platform Software
System Data	(i) usage statistics, system logs, performance and security data, feedback data, records of support requests, and aggregated data about how Our sites, Platform, 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 Account Information where it appears, for example, in log records but excludes Threat Protection Data.

Threat Protection Data	the record of individual User email behaviour and associations formed from the processing, collection and analysis of email metadata such as date and time, sender and recipient email addresses, and other unique message identifiers, but excluding Account Information and System Data.
User	an employee or contractor of a Customer who is authorised by the Customer to access and use the Platform and Services.

Retention Policy **Content**

Data Type	Retention Period	Justification
Webform	This is dependent on the Customer's requirements and how it wishes to receive the submissions. This can be via Secure Email and/or Large File Transfer and/or Workspace – see below for more details.	These are determined by the destination. No data is stored by the webform service after it has been processed.
Secure Email (incl. G-Suite extension) (formerly Switch Secure Email)	**90 calendar days** from the date that the data is received by or last accessed on the Egress Web Access servers. **Note**: this applies each time that the data is received (e.g. each time an email is forwarded or replied to this creates a new Secure Email package that is processed and retained for 90 days).	This ensures that recipients accessing Content on the reader services have a copy of the data for the service to decrypt for it to be viewed. This data is retained in this way to enable the Group to perform its contract with the Customer, User or recipient (as applicable).
Large File Transfer	**90 calendar days** from initial transfer or last package access (unless a shorter/longer period is requested and justified by a Customer).	This ensures that recipients accessing Content on the transfer services have a copy of the data for the service to decrypt. The length can be increased or decreased at Customer request as the neither sender or recipient have a copy of the data. This data is retained in this way to enable the Group to perform its contract with the Customer, User or recipient (as applicable).
Vault	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	Acting as a long-term archive, Customers should set their own retention policy as to how long their organisation should store their Content in this service. This data is retained in this way to enable the Group to perform its contract with the Customer.
Workspace	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	Acting as a long-term file store, Customers should set their own retention policy as to how long their organisation should store their Content in this service. This data is retained in this way to enable the Group to perform its contract with the Customer.

Retention Policy **Threat Protection Data**

Data Type	Retention Period	Justification

Threat Protection Data	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	This data is required to enable the Threat Protection product to improve its accuracy in relation to the Customer and its Users. This is retained for performance of the Group's contracts with Customers, and for its own legitimate interests in preventing fraud and other security risks, and complying with its legal obligations.

Retention Policy **Audit Data**

Data Type	Retention Period	Justification
Secure Email	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	These are retained to enable Customers to review audit logs and ensure access to the services that they've purchased is set correctly. These are retained for performance of the Group's contracts with Customers, and for its own legitimate interests in providing secure services to its Customers.
Large File Transfer	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	These are retained to enable Customers to review audit logs and ensure access to the services that they've purchased is set correctly. These are retained for performance of the Group's contracts with Customers, and for its own legitimate interests in providing secure services to its Customers.
Vault Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	These are retained to enable Customers to review audit logs and searches. These are retained for performance of the Group's contracts with Customers, and for its own legitimate interests in providing secure services to its Customers.
Workspace Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter.	These are retained to enable Customers to review audit logs and ensure access is set correctly. These are retained for performance of the Group's contracts with Customers, and for its own legitimate interests in providing secure services to its Customers.

Where the Group stores Content, any remaining Content, Audit Data and Threat Protection Data is deleted **30 calendar days** after termination or expiry of the Customer's agreement with the relevant Group company unless: (i) a Customer has required that the Group continues to store one or more of them (and has both paid applicable fees and provided the relevant Group company with a written statement outlining the lawful basis for it to do so on the Customer's behalf signed by an authorised signatory of the Customer); or (ii) the Group, or a Group company, is required to retain copies of one or more of them for legal or regulatory reasons. Content may also continue to be stored and processed by the Group where it forms part of another User's or Customer's Content.

Retention Policy **Account Information**

Data Type	Retention Period	Justification
Customer Account Information Relating to the **Customer** (e.g. name, key contact names and contact information, total value of business purchased, functionality purchased, date of joining, date and reason for leaving, correspondence and activity logs) Held in the Group's CRM platform	**10 years** after the Customer's contract with the relevant Group company ends. Key contact names, contact information, correspondence and activity logs will be deleted 5 years after the date of last activity.	This data is retained for business insight, auditing and appropriate financial management purposes in accordance with industry practice. This data is retained in this way for the Group's legitimate interests in undertaking prudent financial, audit, commercial management and record keeping.
User Account Information Relating to the **User** (e.g. name, address, email address, employer Customer)	After the Group's contract with the User's employer (the Group's Customer) comes to an end, the User's account reverts to free user status and the retention period for that user type set out below applies.	This data is retained in this way for the Group's legitimate interests in undertaking prudent and appropriate relationship management activities whilst a Customer exits its contract with the Group. The change to free user status is to ensure continuity of access to packages, both to the user concerned and other recipient users.
Free Users of Egress Accounts (formerly Switch Accounts with Switch IDs)	Free users remain active on our systems for an indefinite amount of time, unless a user raises a request to have their account removed.	This data is held in this way to ensure that the Group can perform its contract with all users by enabling them to access all packages that have previously been sent to them. This is also held to support the Group's legitimate interests in providing and maintaining a platform that enables it to perform services requested by customers and users.
Closed Egress Accounts (formerly Switch Accounts with Switch IDs)	We will retain limited information for **6 years** to show that we actioned the request.	This data is retained in this way to both action a User's request to close or erase their account, and to evidence our compliance with their request. This information is retained for compliance with a legal obligation and for our legitimate interests. The principle of data minimisation is recognised and applied in respect of any data retained.

Retention Policy **System Data**

Data Type	Retention Period	Justification
Logs (System)	Deleted after **1 year** **Note:** Customers can request that these are kept for longer e.g. for meeting regulatory requirements. This will be agreed on a case-by-case basis with the requesting Customer.	These are retained for troubleshooting, identifying recurring trends, prevention of fraud and other security purposes. These are retained to enable performance of the Group's contracts with Customers, and for its own legitimate interests in preventing fraud and other security risks, and complying with its legal obligations.
Logs (Application)	Deleted after **1 year** **Note:** Customers can request that these are kept for longer e.g. for meeting regulatory requirements. This will be agreed on a case-by-case basis with the requesting Customer.	These are retained for troubleshooting and identifying recurring trends. These are retained to enable performance of the Group's contracts with Customers, and for its own legitimate interests in preventing fraud and other security risks, and complying with its legal obligations.
Threat Protection Logs	Deleted after **1 year** **Note:** Customers can request that these are kept for longer e.g. for meeting regulatory requirements. This will be agreed on a case-by-case basis with the requesting Customer.	These are retained for troubleshooting and identifying recurring trends. These are retained to enable performance of the Group's contracts with Customers, and for its own legitimate interests in preventing fraud and other security risks, and complying with its legal obligations.
ZenDesk Support Tickets and Chat history	**6 years** from last update of chat record.	This information is retained to enable the Group to learn from previous activity, and to enable continuity of service if a Customer or user quotes a support ticket reference in future correspondence. This data is retained in this way for the Group's legitimate interests of providing support on its platform and services, and enabling good and consistent customer service.

Retention Policy **Encryption Keys**

Solution Type	Retention Period	Justification
On-Premise Customer solutions	Defined by the Customer	This is setup in accordance to Customer requirements.

Fully hosted Customer solutions	Indefinitely (unless the Customer expressly requests deletion of encryption keys)	This is setup in accordance to Customer requirements. Encryption keys are kept for an indefinite amount of time (unless requested otherwise by the Customer) to allow access to historic packages to/from other recipients of the relevant service.

Encryption keys for partially hosted Customer solutions will follow either one of the above retention policies dependant on the specific key location.

Encryption keys are kept for an indefinite amount of time (unless requested otherwise by the Customer) to allow access to historic packages to/from other recipients of the relevant service.

Retention Policy **Legal or Regulatory**

The Group and its companies may retain copies of a Content, Audit Data and Threat Protection Data where there is a legal or regulatory requirement to do so. Content may also continue to be processed by the Group where it forms part of another User's or Customer's Content.

Retention Policy **Third Party Sub-Processors**

Third-party sub-processor	Retention Period	Justification
Amazon Web Services	Scheduled snapshots are kept for **2 calendar days.** On demand snapshots are kept for up to **30 calendar days.**	Scheduled (Daily) snapshots are kept to restore service in the event of a failure. On demand snapshots are created during maintenance and/or troubleshooting.
Microsoft Azure	Scheduled snapshots are kept for up to **30 calendar days.** On demand snapshots are kept for up to **30 calendar days.**	Scheduled (Daily) snapshots are kept to restore service in the event of a failure. On demand snapshots are created during maintenance and/or troubleshooting.
UK Cloud	Only one snapshot can exist at any one time. This is kept for a maximum of **30 calendar days** (unless another snapshot is taken within that period).	Snapshots are created during maintenance and/or troubleshooting.
UK Fast	Scheduled snapshots are taken daily and only kept until the next snapshot is taken the following day. On demand snapshots are kept for a maximum of **7 calendar days**.	Scheduled (Daily) snapshots are kept to restore service in the event of a failure. On demand snapshots are created during maintenance and/or troubleshooting.
CommuniGator	Data is removed from the platform **one month** after completion of marketing campaign.	This is required for the successful deliver email campaigns to Customers or potential Customers who have requested marketing information.
Server Choice (Bulletproof)	Logs sent to Bulletproof as part of the Group's (Internal) SIEM solution are retained for up to 1 year.	This is required to help in the assistance of an investigation and performance review.

Retention Policy **Destruction of Data**

We and our Group are aware of our obligations under the GDPR. As a result, our policy is that upon expiry of an applicable retention period, any relevant information and personal data must be **irretrievably deleted and destroyed in a secure manner** in compliance with the GDPR and appropriate regulatory guidance.

Furthermore, below we have identified the measures that are taken by our Third Party Sub-Processors who host underlying infrastructure (such as Virtual Machines) and the measures that they take regarding the destruction of data.

Third-party sub-processor	Method of Deletion	External References
Amazon Web Services	From AWS: Overview of Security Processes (May 2017) p.6: "When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process."	https://bit.ly/2xGkL9w See p.23 for details on EC2 and EBS, p.24,28-29 for details on isolation, and p.45-47 for details on S3.
Microsoft Azure	From Protecting Data in Microsoft Azure (August 2014), Section 3.3 (p.16) referring to default protection: "Where appropriate, confidentiality should persist beyond the useful lifecycle of data. The Azure Storage subsystem makes customer data unavailable once delete operations are performed. All storage operations including delete are designed to be instantly consistent."	https://bit.ly/1UBJW5U See Section 3.5 for more details on Data Deletion (p.21-22).
UK Cloud	UK Cloud use deletion methods assessed and validated by NCSC to ensure that data is zeroed and cannot be recovered. At the point of termination or replacement of physical assets, UK Cloud ensure that these are both sanitised to IAS5 standards and then securely disposed of by SC Cleared staff members.	Confirmed by vendor.
UK Fast	All content will be securely deleted to HMG standards and data disks will be securely stored from this point until their destruction, performed at UK Fast. Audits of this can be requested from UK Fast.	Confirmed by vendor.

Changes to this Policy **Transparency**

Version	Release Date	Changes to previous version
1.04	24 May 2018	Launch of policy in current form.
1.05	3 July 2018	▪ Introduced definitions of Group, Software, Plug-Ins, Platform Software, System Data and Threat Protection Data. ▪ Adjusted definition of Customer to include those purchasing through a managed service provider or reseller. ▪ Included references to Threat Protection Data and Audit Data in paragraph under Audit Data table, and clarified that Content retention only applies where the Group stores Content. ▪ Minor layout changes.
1.06	24 Jan 2019	▪ Clarified on page 8 that Microsoft Azure Scheduled snapshots are kept for “up to” 30 days

Egress Software Technologies

Egress Software Technologies is the leading provider of information security services designed to secure shared data from start to finish using a single platform: Egress.

The Egress platform is made up of highly integrated and flexible service lines. These award-winning services include email and document classification, the only email and file encryption product to be CPA certified by NCSC, secure managed file transfer, secure online collaboration and secure archive.

www.egress.com

info@egress.com

0844 800 0172

@EgressSoftware