Data Retention Policy

Our Services

Version 1.11 (9 September 2020)

1 Policy definitions

The following terms are used in this Policy:

Audit Logs	recorded privileged actions performance by named and/or authenticated accounts against Customer Content. The content of audit events is variable by subject matter and context.
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 you, Users and Recipients, including any Personal Data in it. It does not include CRM Information, Smart Data or System Data.
CRM Information (formerly Account Information)	the databases, logs and other collections of Personal Data about you and your Users that is provided to Us by you, your Users, or that We obtain in connection with: (a) the creation and administration of accounts; (b) how the Services, Software and Support are used, accessed and interacted with; (c) any permissions, consents or preferences; and (d) you being Our customer, and information that We obtain from third parties that may be linked to you or your organisation.
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 (including Egress Software Technologies, Inc (a Massachusetts corporation, registered office: Suite 2, Level 3, 268 Summer Street, Boston MA 02210, United States).
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 services and associated functionality which are delivered either as a fully-hosted, partially-hosted or on-premise model and which include the use of, or access to, the Software.
On-Premise Software	any part of the Software necessary to enable you to host all or part of the Services on your infrastructure.
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	the Group's proprietary services and associated functionality which are delivered either as a fully-hosted, partially-hosted or on-premise model and which include the use of, or access to, the Software.
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.
Software	collectively Plug-Ins and On-Premise Software
System Data	security data, feedback data, records of support requests, and aggregated data about how Our 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 (b) 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.
User	an employee or contractor of a Customer who is authorised by the Customer to access and use the Platform and Services.

2 Service Data Retention Periods

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 Secure Workspace – see below for more details.	These are determined by the destination. No data is stored by the Webform service after it has been successfully processed and delivered to the receiving system.
Protect (formerly Secure Email, 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 nor 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).
Investigate (formerly e-Discovery & Analytics, and Vault)	For the duration of the Customer's agreement with the relevant Group company, and for up to **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.
Secure Workspace	For the duration of the Customer's agreement with the relevant Group company, and for up to **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.

Smart Data

Data Type	Retention Period	Justification
Smart Data Relevant to Prevent (formerly Risk Based Protection, and 'Threat Protection')	For the duration of the Customer's agreement with the relevant Group company, and for up to **30 calendar days** thereafter.	This data is required to enable the Prevent and Smart Authentication services to improve their accuracy. This is retained for performance of the Group's contracts with Customers, and for its own legitimate interests in providing secure services to its Customers. It is also retained for preventing fraud and other security risks, and complying with its legal obligations.

Dedicated Egress Secure Infrastructure (ESI)

Location	Retention Period	Justification
Dedicated hosted ESI	For the duration of the Customer's agreement with the relevant Group company, and for up to **30 calendar days** thereafter.	This is maintained in this manner as once deleted, no previously encrypted emails will be accessible either for the Customer or for any of their 3rd party recipients. This provides time for Content to be decrypted and downloaded prior to deletion.
Dedicated on-premise ESI hosted by the customer	Not applicable as the Group is not in control of hosting this Service. The Group will revoke the Customer's federation certificate promptly following expiring or termination of the Customer's agreement with the relevant Group company which will disable use of the ESI Service.	The Group revokes the federation certificate in order to prevent continued use of the Service after the relevant Customer's subscription period has expired or been terminated by either party.

Audit Logs

Data Type	Retention Period	Justification
Secure Webform Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for **30 calendar days** thereafter. For hosted ESIs these are retained until the Customer's instance is decommissioned following expiry or	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.

	termination of their agreement with the relevant Group company.	
Protect Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for 30 calendar days thereafter. For hosted ESIs these are retained until the Customer's instance is decommissioned following expiry or termination of their agreement with the relevant Group company.	These are retained to enable Customers to review audit logs and ensure access to the services that they have 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 Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for 30 calendar days thereafter. For hosted ESIs these are retained until the Customer's instance is decommissioned following expiry or termination of their agreement with the relevant Group company.	These are retained to enable Customers to review audit logs and ensure access to the services that they have 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.
Investigate Audit Logs (formerly e-Discovery & Analytics, and Vault)	For the duration of the Customer's agreement with the relevant Group company, and for 30 calendar days thereafter. For hosted ESIs these are retained until the Customer's instance is decommissioned following expiry or termination of their agreement with the relevant Group company.	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.
Secure 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.
Prevent Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for 30 calendar days thereafter.	These are retained in order to enable the Group to demonstrate why the system behaved in the way it did upon yielding advice to the Customer.

Where the Group stores Content, any remaining Content and Audit 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.

3 CRM Information Retention Periods

Data Type	Retention Period	Justification
Customer CRM Information Held in the Group's Salesforce instance and 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)	**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 unless the Customer is an individual online subscriber when they will be kept for as long as required to by law (e.g. to meet financial reporting and audit requirements).	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 CRM 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

Data Type	Retention Period	Justification
		recognised and applied in respect of any data retained.

4 System Data Retention Periods

Logs

Data Type	Retention Period	Justification
Logs (System)	Up to **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. If you purchase SIEM, then these logs will be retained for a year.	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 **30 days** **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. If you purchase SIEM, then these logs will be retained for a year.	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.
Prevent Application Logs	Deleted after **90 days** **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.

Encryption Keys

Deployment Type	Retention Period	Justification
On-Premise Customer deployments	Defined by the Customer	This is setup in accordance to Customer requirements.
Fully hosted Customer deployments	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.

Mobile App Logs

Data Type	Retention Period	Justification
Logs (System)	Up to **90 days** **Note:** these logs are created by our app based on information provided by the Group's Egress Secure Infrastructure (ESI) system. They are generated and returned based on user actions within our app.	These are retained for troubleshooting, identifying recurring trends, prevention of fraud and other security purposes. These enable the Group's performance of its contracts with Customers and Users, and for its own legitimate interests in preventing fraud and other security risks within its services and software, and complying with its own legal obligations.

5 Legal and Regulatory Retention

The Group and its companies reserve the right to retain information as may be required by a legal or regulatory requirement or order to do so.

6 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.
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.
Twilio, Inc.	2 factor authentication SMS requests are kept for **30 calendar days** before being overwritten	This is maintained for a limited time in order to provide an audit record of MFA requests that may be reviewed in the event of a data security incident.
Mailgun Technologies, Inc.	Message bodies are retained for up to **72 hours**. Message metadata (including sender, recipient('s), subject and source IP) is retained for **30 days**.	This is required for outbound mail notifications from various platforms. Data is retained to enable re-sending messages on failure, and diagnosing issues in mail relaying.
CalliTech Limited	The limited information collected to provide the overflow call service is retained by CalliTech Limited whilst it is required to deliver the service to us.	Provides overflow support call services, and transfer out-of-hours support calls to our engineers.
Zoom Video Communications Ltd	For the period necessary to fulfil the purposes outlined in its privacy notice (unless a longer period is required by law). See more at: https://zoom.us/privacy	Used to facilitate calls between the Group's employees and between Group and its Customer's.
Zendesk	**6 years** from last update of chat record.	Provides support ticket and online chat software and services used by us to provide support to all of our customers and users.

7 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	"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	"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

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
1.07	16 July 2019	▪ Updated Account Information references to CRM Information to reflect recently launched Master Subscription Agreement. ▪ Updated Threat Protection references to Smart Data to reflect recently launched Master Subscription Agreement. ▪ Updated references to Vault to e-Discovery and Analytics to reflect new service name. ▪ Updated references to Workspace to Secure Workspace to reflect new service name. ▪ Updated retention policy for Smart Data to accurately reflect the way that learned behaviour is ingested by the machine learning and AI software that underpins Risk Based Protection and Smart Authentication in order to provide the service to Customers and Users and the businesses that they interact with.
1.08	31 October 2019	▪ Updated to include details of data retention by Twilio, Inc. which provides the multi-factor authentication SMS on some Group products and services. ▪ Updated details around Webform and Workspace Content retention. ▪ Added details relating to RBP, Data Platform and Webform Audit Logs ▪ Added details relating to Audit Log retention on hosted ESIs
1.09	27 March 2020	▪ Introduced definition of "Audit Logs" ▪ Adjusted the justification for Webform Content to reflect that no data is retained after it has been successfully processed and delivered. ▪ Clarified the Services that Smart Data is relevant to. ▪ Changed Section Heading from "Audit Data" to "Audit Logs" ▪ Included details around hosted ESI audit log retention. ▪ Included details around Secure Webform and RBP Audit Log retention.

		▪ Clarified retention period of System Logs, and shortened retention period of Application Logs and RBP Application Logs. ▪ Included additional detail around Third-Party Processors - Twilio, Inc., Mailgun Technologies, Inc., CalliTech Limited (MoneyPenny), Zoom Video Communications, Inc. and Zendesk Inc.
1.10	27 July 2020	▪ Clarified the retention period of Smart Data
1.11	9 September 2020	▪ Clarified that retention periods relevant to Investigate, Secure Workspace and Smart Data are "up to" 30 days. ▪ Introduced detail about the retention of access to Dedicated Egress Secure Infrastructure (ESI). ▪ Clarified retention of CRM information relating to individual online subscribers. ▪ Clarified impact of purchasing SIEM on retention of Application and System logs

Egress Software Technologies Ltd

Egress provides human layer security – helping users receive, manage and share sensitive data to meet compliance requirements and drive business productivity.

Egress' award-winning platform makes sure emails and files are delivered to the correct recipient, encrypts and protects sensitive data, and provides compliance auditing and reporting.

www.egress.com

info@egress.com

0844 800 0172

@EgressSoftware