Data Retention Policy

Our Services

Version 1.19 (May 2023)

1 Policy definitions

The following terms are used in this Policy:

Add-Ins	one or more proprietary software or Third-Party Software components, add-ins or apps provided by our Group for installation onto a Customer's network and infrastructure, or User devices in order to access and use the Services.
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 and Software by you, Users and recipients, including any Personal Data in it. It does not include CRM Information, Smart Data, Threat Data, Third-Party Data or System Data.
Content of Concern	Content that is likely to cause harm, distress, or alarm as set out in local legislation (such as the UK Online Safety Bill).
CRM Information	Information on the Group's customer relationship management databases relating to a Customer's business and the Group's relationship with it.
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 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: One Marina Park Drive, Suite 1410, Boston MA 02210, United States); Egress Software Technologies Inc (an Ontario corporation, registered office: 30 Via Renzo Drive, Suite 200, Richmond Hill, L4S 0B8, Ontario, Canada); Egress Software Technologies Limited (a foreign legal entity registered on the Dutch Chamber of Commerce, number: 74110462, registered office: Herengracht 420, 1017 BZ Amsterdam, The Netherlands); and, Egress Software Technologies Pty Ltd (an Australian company, ACN: 667 428 971, registered office: Spaces, 80 Ann Street, Brisbane, Queensland 4000, Australia).
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.
On-Premise Software	any part of the Software necessary to enable a Customer to host all or part of the Services on its networks and infrastructure.
Plug-Ins	one or more proprietary software or Third-Party Software components, plug-ins or apps provided by our Group for installation onto a Customer's network and infrastructure, or

Copyright © Egress Software Technologies Ltd. All rights reserved.

	User devices in order to access and use the Services.
Services	the Group's services delivered either as a fully-hosted, partially-hosted or on-premise model and including the use of, or access to, the Software. This term does not include any professional services delivered by or on behalf of a member of our Group.
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 and Third-Party Data. This excludes CRM Information, Threat Data and System Data.
Software	the software that enables the Group to deliver, develop, enhance and provide the Services, including the Plug-Ins, On-Premise Software, Third-Party Data and Third-Party Software.
System Data	security data, feedback data, records of support requests, and aggregated data about how the Group's 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 excludes Content, Smart Data and Threat Data.
Third-Party Data	data that is proprietary to third-parties that the Group receives and which may be included in the data sets processed by the Services to enable them to operate in the way described.
Third-Party Software	software that is proprietary to third-parties that the Group licences and which may be included within the Services to provide additional functionality.
Threat Data	data identified by the Services as, without limitation: (a) malicious; (b) indicative of cyberattack or other threat; or (c) that which is, or could be, used to exploit vulnerabilities, conduct malicious activity, malware or ransomware infections, data theft or unauthorised access, cyberattacks or other activity. Threat Data includes data derived from the foregoing.
User	an employee or contractor of a Customer who is authorised by the Customer to access and use the Services.

Copyright © Egress Software Technologies Ltd. All rights reserved.

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	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 agreement with the Customer, User or recipient (as applicable).
Large File Transfer	Default period of 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 agreement with the Customer, User or recipient (as applicable).
Respond (formerly Investigate, 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 agreement 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

Copyright © Egress Software Technologies Ltd. All rights reserved.

Data Type	Retention Period	Justification
		the Group to perform its agreement with the Customer.

Smart Data

Data Type	Retention Period	Justification
Smart Data Relevant to Prevent and functionality within the Egress Security Center	18 months rolling, and for up to 30 calendar days thereafter.	This data is required to enable the Prevent and Smart Authentication Services to improve their accuracy. It is also used to provide trend and risk analysis for reporting to Customers and their applicable Users through functionality within the Egress Security Center. This is retained for performance of the Group's agreements 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.

Threat Data

Data Type	Retention Period	Justification
Threat Data Relevant to Defend and functionality within the Egress Security Center	18 months for access to in-depth classification through email specific dashboard.	This data is required to enable Defend to deliver risk alerts, and inform users why a risk has been scored. It is also used to provide trend and risk analysis and reporting for Customers and their applicable Users through functionality within the Egress Security Center.
Threat Data Relevant to Defend and functionality within the Egress Security Center	50 years retention of email addresses confirmed as malicious.	This is retained for performance of the Group's agreements with Customers, and for its own legitimate interests in providing secure Services to its Customers and ensuring that new threats are identified and responded to accordingly by the Defend Service. It is also retained for preventing fraud and other security risks, and complying with its legal obligations

Copyright © Egress Software Technologies Ltd. All rights reserved.

Threat Data Relevant to Defend and functionality within the Egress Security Center	The interaction between two email addresses is retained for the duration of the Customer's agreement with the relevant Group company, and for up to 30 calendar days thereafter.	This is retained for performance of the Group's agreements with Customers and for its own legitimate interests in providing secure Services to its Customers and ensuring that new threats and malicious emails are identified and responded to accordingly by the Defend Service. The interaction between two email addresses is also used to provide trend and risk analysis and reporting for Customers and their applicable Users through functionality within the Egress Security Center.

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	These are retained to enable Customers to review audit logs and ensure access to the Services that they have purchased is set correctly. They are also retained for performance of the Group's agreements with Customers, and for its own legitimate interests in

Copyright © Egress Software Technologies Ltd. All rights reserved.

Data Type	Retention Period	Justification
	following expiry or termination of its agreement with the relevant Group company.	providing secure Services to its Customers.
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 its 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. They are also retained for performance of the Group's agreements 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. They are also retained for performance of the Group's agreements with Customers, and for its own legitimate interests in providing secure Services to its Customers.
Respond 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 its agreement with the relevant Group company.	These are retained to enable Customers to review audit logs and searches. They are also retained for performance of the Group's agreements 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 to the Services that they have purchased is set correctly. These are retained for performance of the Group's agreements 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	These are retained in order to enable the Group to demonstrate why the system behaved in the way it did upon yielding

Copyright © Egress Software Technologies Ltd. All rights reserved.

Data Type	Retention Period	Justification
	90 calendar days thereafter.	advice to the Customer.
Defend Audit Logs	For the duration of the Customer's agreement with the relevant Group company, and for 90 calendar days thereafter.	These are retained in order to enable the Group to correlate user activity and support any security events.

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.

Copyright © Egress Software Technologies Ltd. All rights reserved.

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 agreement 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 agreement 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 agreement 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. Customers can request that these Users are deleted and do not revert in this way (any such request must be made during the termination and decommissioning process). Any such request will prevent recipients from accessing any packages associated with such a deleted User.
Complaints	2 years after last activity. 7 years if it relates to the exercise or defense of legal claims.	This helps meet legislative requirements in some jurisdictions and enables.
Free Users of Egress	Free users remain active on the	This data is held in this way to

Copyright © Egress Software Technologies Ltd. All rights reserved.

Data Type	Retention Period	Justification
Accounts (formerly Switch Accounts with Switch IDs)	Group's systems for 7 years from last activity, unless a user raises a request to have their account removed prior to this date.	ensure that the Group can perform its agreements 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)	The Group will retain limited information for 6 years to show that it has 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 the Group's compliance with their request. This information is retained for compliance with a legal obligation and for the Group's legitimate interests. The principle of data minimisation is recognised and applied in respect of any data retained.

Copyright © Egress Software Technologies Ltd. All rights reserved.

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 agreements with Customers, and for its own legitimate interests in preventing fraud and other security risks within its Services and Software, 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 agreements with Customers, and for its own legitimate interests in preventing fraud and other security risks within its Services and Software, 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 agreements with Customers, and for its own legitimate interests in preventing fraud and other security risks within its Services and Software, and complying with its legal obligations.
Defend Application Logs	Deleted after 90 days	These are retained for troubleshooting and identifying issues such as failures/restarts, data connection events and other service operational events.

Copyright © Egress Software Technologies Ltd. All rights reserved.

Salesforce Support Tickets and Chat history	6 years from last update of support case.	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 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 set-up in accordance to Customer requirements.
Fully hosted Customer deployments	Indefinitely (unless the Customer expressly requests deletion of encryption keys)	This is set-up 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 the Egress app based on information provided by the Group's Egress Secure Infrastructure (ESI) system. They are generated and returned based on user actions within the Egress app.	These are retained for troubleshooting, identifying recurring trends, prevention of fraud and other security purposes. These enable the Group's performance of its agreements with Customers and Users, and for its own legitimate interests in

Copyright © Egress Software Technologies Ltd. All rights reserved.

		preventing fraud and other security risks within its Services and Software, and complying with its own legal obligations.

Copyright © Egress Software Technologies Ltd. All rights reserved.

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.

Reports of Content of Concern

Data Type	Retention Period	Justification
Information collected by the reporting tool or process	3 years Due to the nature of the Services, the Group may not be able to view reported Content, make any assessment, or take any action itself. Instead, if a link is provided, the Group may be able to identify the relevant customer or user and share the report to them (without identifying the reporter).	The data collected by the Group's form or processes does not include information which may identify the reporter. A copy of the report is kept for this period to enable the Group to comply with the request and to report it to other relevant parties (e.g. the customer or user responsible, where this is possible). Aggregated details, including the number, date and type of requests, are kept indefinitely.

Content of Concern

Data Type	Retention Period	Justification
Content	Deleted where appropriate following review. If a decision is taken not to delete the reported Content, then the retention period set out above in relation to Content will continue to apply.	Where the Group receives a report of Content of Concern it will either investigate the relevant Content itself (where it is the Controller), or, where it is not the Controller, it will where possible and not prohibited by law, notify the relevant Data Controller. If the Group is responsible, it will investigate the Content of Concern and decide whether or not it should be deleted. If a customer or user is responsible, they will also be responsible for any investigation and subsequent actions.

Reports of Intellectual Property Rights infringement (including under DMCA)

Data Type	Retention Period	Justification
Information collected by the webform	3 years Due to the nature of the Services, the Group may not be able to view	A copy of the report is kept for this period to enable the Group to comply with the request and to report it to other relevant parties (e.g.

Copyright © Egress Software Technologies Ltd. All rights reserved.

	reported Content, make any assessment, or take any action itself. Instead, if a link is provided, the Group may be able to identify the relevant customer or user and pass on the report to them.	the customer or user responsible, where this is possible). Aggregated details, including the number, date and type of requests, are kept indefinitely.

Copyright © Egress Software Technologies Ltd. All rights reserved.

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.
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 the Group.	Provides overflow support call services, and transfer out-of-hours support calls to the Group's engineers.
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.
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.
SalesForce Service Cloud	6 years from last update of support case.	Provides support ticket and online chat software and services used by the Group to provide support to all of its Customers and Users.
Security Information and Event Management (SIEM)	Logs sent to the Group's 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.
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 Customers.

Copyright © Egress Software Technologies Ltd. All rights reserved.

7 Destruction of Data

The Group's 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 the Group has identified the measures that are taken by its 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."*	Data Layer - Amazon Web Services (AWS). See for details on EC2 S3 deleted to NIST 800-88 standard.
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."*	ISO/IEC 27018 - Azure Compliance | Microsoft Docs. Deletion carried out to ISO 27018 standard.
MongoDB Atlas	*"If a customer terminates an Atlas cluster, the following happens: it will become unavailable immediately; MongoDB, Inc. may retain a copy of the data for up to 5 days; the backup associated with the managed cluster is also terminated. If a customer terminates backup, all snapshots become unavailable immediately. It may take up to 24 hours for all copies of the data to be deleted."*	Atlas Security document

Copyright © Egress Software Technologies Ltd. All rights reserved.

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.

Copyright © Egress Software Technologies Ltd. All rights reserved.

		▪ 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
1.12	01 July 2021	▪ Extended Prevent audit retention to 90 days for support investigations ▪ Added Defend ▪ Replace Zendesk with SalesForce as support subprocessor
1.13	8 September 2021	▪ Updated details on effect on Users on termination of a business account ▪ Improved the descriptions of Defend retention ▪ Removed references to "Platform" and the associated definition as it is replaced by the references to "Services" ▪ Updated definition of CRM Information to be consistent with the Group's Service Retention Policy on its website ▪ Removed UKFast.Net Limited from Section 6.
1.14	13 September 2022	▪ Updated definitions to reflect current Egress Master Subscription Agreement ▪ Updated retention of free users to be 7 years, replacing the previous reference to indefinite. ▪ Revised data destruction links for third-party hosts in Section 7 ▪ Added definition for 'Content of Concern' ▪ Added retention periods in Section 5 for reports of Content of Concern and allegations of Content which infringes intellectual property rights.
1.15	01 December 2022	▪ Separated Defend Audit and System retention periods
1.16	March 2023	▪ Updated US office address ▪ Changed retention period of email addresses identified as malicious by Defend from indefinite to 50 years ▪ Introduced retention period for complaints
1.17	March 2023	
1.18	April 2023	▪ Removed UK Cloud as a Sub-Processor from Sections 6 and 7 ▪ Changed defined term of "Plug-In" to "Add-In" for consistency with updated MSA v3.12 (April 2023)
1.19	May 2023	▪ Added greater clarity around retention of Threat Data by breaking it out different parts.

Copyright © Egress Software Technologies Ltd. All rights reserved.

		▪ Changed part of Threat Data retention from 40 days to 18 months to enable better reporting and analysis functionality within the Egress Security Center. ▪ Added clarity to the Justification column for Smart Data, Threat Data and Prevent, Protect and Defend logs to explain that these may also be retained in order to deliver reporting and analysis functionality within the Egress Security Center. ▪ Added details of our new Australian subsidiary into the definition of Group.

Copyright © Egress Software Technologies Ltd. All rights reserved.

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

Copyright © Egress Software Technologies Ltd. All rights reserved.