Law enforcement **Guidelines for making requests**

This document is intended for use by law enforcement bodies who are seeking disclosure of information from a member of the Egress Software Technologies Group. The relevant members of the Group as at **April 2019** are:

- Egress Software Technologies Limited, a United Kingdom company
- Egress Software Technologies Limited, a foreign company registered on the Dutch Chamber of Commerce
- Egress Software Technologies, Inc., a Massachusetts corporation, United States.
- Egress Software Technologies Inc, an Ontario corporation, Canada.

We refer to all of the above collectively in this document as the **Group**.

Types of information

Content	the files, data, text, audio, video, images and other materials that are transferred, stored, shared or hosted on or through the Group's 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.
CRM Information	the databases, logs and other collections of personal data about customer and users that is provided to the Group by customers, users, or that the Group obtains in connection with: (i) the creation and administration of accounts; (ii) how its services, software and support are used, accessed and interacted with; (iii) any permissions, consents or preferences; and (iv) customers and users being Group customers, and information that the Group obtains from third parties that may be linked to customers, users or their organisations.
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.
System Data	(i) usage statistics, system logs, performance and security data, feedback data, records of support requests, and aggregated data about how Group 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.

The Group makes a distinction between requests it receives for disclosure of **Content** as opposed to requests for disclosure of other information and data. The Group:

- will disclose non-Content information only in response to valid and binding legal requests.
- will not disclose Content, access to which is managed by its customers and users. **Content disclosure must be sought from the relevant Group customer or user.**

Law enforcement **Making a request**

Legal Process

The Group requires due legal process to be observed and followed in the relevant jurisdiction(s) and will not release information without a valid and binding legal request properly served on it. Legal requests must:

- correctly identify the relevant Group entity as the service provider the request is made of
- identify the legislation, court order or other authority in reliance on which the request is made
- provide the full name of the relevant Group customer or user to whom the request relates
- provide the name, title and contact information of the person making the request and to whom disclosure is requested
- be made on headed paper of, or sent from an email account at, the law enforcement authority making the request
- be as narrow and specific as possible. **The Group may object to any overly broad or in appropriate request.**

Making a request

All legal requests must be made to the relevant local representative:

UK and the rest of the World		**United States**	
Entity:	Egress Software Technologies Limited	**Entity:**	Egress Software Technologies, Inc.
Address:	12th Floor, The White Collar Factory, 1 Old Street Yard, London, EC1Y 8AF	**Address:**	Suite 2, Level 3, 268 Summer Street, Boston, MA 02210, United States
Attention:	General Counsel	**Attention:**	General Counsel
Copy to:	legal@egress.com security@egress.com	**Copy to:**	legal@egress.com security@egress.com
Canada		**Europe**	
Entity:	Egress Software Technologies Inc	**Entity:**	Egress Software Technologies Limited
Address:	Suite 304, 11685 Yonge Street Richmond Hill, L4E 0K7, Ontario, Canada	**Address:**	Oval Tower, De Entrée 99-19, Amsterdam, 1101 HE, The Netherlands
Attention:	General Counsel	**Attention:**	General Counsel
Copy to:	legal@egress.com security@egress.com	**Copy to:**	legal@egress.com security@egress.com

Requests relating to data held outside of that jurisdiction

Legal requests must follow applicable law. If the legal request relates to personal data or PII held outside the jurisdiction in which the request is served the requestor must follow relevant legal, political and diplomatic channels in that jurisdiction to lawfully and appropriately seek disclosure from the Group (including Mutual Legal Assistance Treaties and The CLOUD Act).

Law enforcement **Points to note**

Preservation requests: The Group will preserve the requested information following receipt of a valid and binding preservation request for 90 days. The Group will only preserve information up to 90 days prior to the date of the request – information produced or created after this date will not be preserved under that request.

Witness Testimony: The Group will not waive legal requirements for subpoenas seeking witness testimony. Upon receipt of a valid and binding legal request the Group will provide a certification of authenticity or regulatory conducted business activity in lieu of witness testimony.

Civil Requests: Civil requests must follow appropriate local legal process. Information, records and testimony requested from the Group in a civil action in a state court in the United States other than the Commonwealth of Massachusetts must follow MGL c. 223A, s.11.

Notifications: Unless prohibited by applicable law, the Group will notify the relevant customer or user before making any disclosure in respect of a valid and binding legal request.

Costs reimbursement: Where permitted by applicable law, the Group reserves the right to seek reimbursement for the costs associated with responding to legal requests. Currently the Group waives all costs associated with responding to emergency requests and requests related to the exploitation of children.

Method of disclosure

When making disclosure in response to a valid and binding legal request, the following principles apply:

- all results will only be provided in PDF format unless otherwise agreed
- the Group will return results via email to the requestor using appropriate secure communication
- if a request requires the production of voluminous results, the Group reserves the right to disclose documents using secure storage solutions
- the Group is not responsible for any blocking of its responsive emails by the requestor's email system (including by any anti-spam email tools). **The requestor must ensure the designated recipient can receive emails from the Group's domain, egress.com**.
- the Group will not send any disclosures to any web-based email address (e.g. Hotmail, Yahoo, or Gmail).