The basics

Who we are

Egress Software Technologies Limited is a company based in the United Kingdom and is the parent company within our group (which means that it owns the other companies). We use the words we, us, and our to refer to our business in this document. You can find out more about us and our group at www.egress.com/about.

What is 'personal data' or 'personal information'

It is difficult to provide a complete definition which applies wherever you are located as the definitions used around the world differ, sometimes quite subtly. Generally it means something akin to information that "relates to an identified or identifiable natural person". As well as personal data/personal information, you may hear other phrases such as sensitive data, NPI (non-public personal information) and PHI (protected health information) and so on. These are specific kinds of personal data that may have additional obligations in relation to how they are stored, shared and processed. In this document we just refer to 'personal data'.

Who holds your information

We store and process your Content and Smart Data on your behalf. These contain personal data. Which company in our group is responsible for this will be set out in your agreement with us which will be either our online subscriber terms or your organisation's contract with us if you are a user within a business account. We describe what we mean by Content and Smart Data a little further down. You can contact us at dpo@egress.com or through our webform to exercise your rights.

We do collect and process some other types of personal data which we also explain below. These are held by Egress Software Technologies Limited. We hold this personal data for and on behalf of ourself and the other companies in our group.

How long we hold your information for

We keep personal data for the periods set out in our data retention policy. You can always find the current version of this document at www.egress.com/legal.

Where your information is stored

The table below explains the different ways that we talk about the data we hold and process. We use this data, which may contain personal data, to run our business and deliver our services to you.

Information you control	What it is / means	Where it is stored
Content	the files, data, text, audio, video, images and other materials that you transfer, store, share or host through use of our service.	UK, EU, US, Australia. If you register online, this is determined by your location at the time you subscribe. If you are a business then you may specify your preference during discussions with us.
Smart Data (specific to our Prevent service)	the record of your individual email behaviour and the associations that you have with recipients that our Prevent service learns from processing, collecting and analysing your email activity, this includes email metadata ('metadata' means data that provides information about other data). It is created by analysing your emails and prompts you before sending an email to review things Prevent thinks may be wrong (e.g. wrong attachment, wrong recipients).	
Information we control	What it is / means	Where it is stored

CRM Information	the information that we hold about our relationship with you (which includes any information shared to assist both of us in resolving any questions or support requests).	UK and EU
System Data	(a) usage statistics, system logs, performance and security data, feedback data, records of support requests, and aggregated data about how our websites, 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, and unsuccessful security incidents).	UK, EU, US, Australia
Threat Data (specific to our Defend service)	Inbound emails and identified data which may be, for example: (a) malicious; (b) indicative of cyberattack or other threat; or (c) capable of use to exploit vulnerabilities, conduct malicious activity, malware or ransomware infections, data theft or unauthorised access, cyberattacks or other activity. This data set includes data that can be derived from these.	UK, EU, US, Australia

Remember, we do not control the countries that you access our services from. When a user responds to your secure email, their response will be stored where their service is hosted (which may not be the same as you).

Selling information

We do not sell or rent your personal data to third-parties. This is a concept that is referred to in a number of State laws in the United States (including California, Colorado, Connecticut, Utah, Virginia and Nevada). Note that 'sale' does not include situations where we disclose personal data at your direction, or when it is otherwise permitted by law.

Security measures

We put a lot of effort into keeping your personal data secure and confidential. It is very important to us. We have technical and organisational measures and tools in place to appropriately protect it. These help prevent accidental, unauthorised, or unlawful access, use, loss, destruction or damage to it. We use administrative (e.g. training our employees on privacy and information security), technical (e.g. pseudonymization or encryption techniques, and the use of firewalls), and physical (e.g. locks and video surveillance at our office premises) measures. Access to your personal data is limited to employees, agents, contractors and third-parties that we have carefully checked. They only have access where they have a business need to do so. They will only process personal data on our instructions and are subject to duties of confidentiality.

Still, no system can be guaranteed to be 100% secure. If you have questions about the security of your personal data, or if you have reason to believe that the personal data that we hold about you is no longer secure, please contact us right away.

The rights you have in your personal data

You can find out about the rights you may have in the personal data that we hold about you here. On that page, you will also find the contact details of our Data Protection Officer.

Opting out of marketing information

If you no longer wish to receive direct marketing emails from us, you may opt out of receiving these emails by clicking on the 'Unsubscribe' link at the bottom of any marketing email you receive.

Doing your part

It is important you make sure the personal data that we hold about you (and if you are a business, your users) is accurate, up-to-date and relevant. Tell us promptly if there are any changes by emailing us here. Please also make sure you are legally able to use our services and to process information through them (in the UK and the EU this is referred to having an identified 'lawful basis').

How your personal data is collected

From you when you

- subscribe to our services
- log into or use your Egress account
- fill out forms on our website or apps
- use our website, apps and services
- communicate with those who use our services (see more on that below)
- contact us
- take part in our competitions and promotions
- attend webinars (we may record our webinars and keep a record of attendees)

From other parties such as

- companies or individuals that introduce you to us (like our partners)
- credit reference agencies
- third-party data providers who we purchase information from
- publicly accessible records
- government and law enforcement agencies
- Microsoft where, if you use our add ins, you grant us permission to access each email you send or receive in order to encrypt or decrypt it (if you use Protect), process Smart Data (if you use Prevent) and/or Threat Data (if you use Defend)

From other parties who

- use our services
- fill out forms on our website or apps and provide personal data about you
- contact us and provide personal data about you
- fill out forms on websites or webforms that we host on behalf of one of our customers

From cookies

You can find out more about the cookies on we use on our website in our Cookie Policy. For information about cookies that we use to deliver our services, check out our Product Cookie Policy. Some web browsers may transmit "do-not-track" signals to the websites and online services you communicate with. Whilst there is no industry standard that governs what, if anything, we should do if we receive such a signal, our website will not set cookies if your browser is set to 'do-not-track'.

IP addresses

When you visit our website, apps or use our services we record your IP address. This may be kept in log files or matched against public or proprietary databases to provide us with information about your visit. It may identify the organisation to whom the IP address is registered (and in some cases enable us to identify you).

Remember, if you communicate with us and with organisations that use our services

Your emails and their associated metadata will be routinely monitored to protect against outbound risk (such as misaddressed emails), inbound risk (such as phishing) and to improve the accuracy of the guidance provided by our services. This monitoring may include the processing of certain information about you (e.g. the strength of your association with the sender/recipient, and the trustworthiness of your domain).

Lastly, you may provide us with information about other people….

This could be Content which belongs to another person. You must make sure you have the rights and permission to do so. By providing it, or sending it via or uploading it to our services, you confirm that you do.

How we use your personal data

We use the data that we collect for a few reasons, examples of which are given below.

Managing our relationship with you and/or your organisation

- communicating with you
- retaining appropriate financial and business records
- contacting you in relation to potential sales opportunities, and to understand you and/or your organisation better
- creating reports or profiles for marketing and analytics purposes
- contacting you and any relevant regulator in the event of a data breach where required to do so

Delivering our services

- providing our service access and support to you
- providing guidance on our services
- responding to, and resolving, complaints, queries, requests and support tickets
- ensuring our services are working properly
- pro-active maintenance and investigations
- alerting you to issues or updates to the services you subscribe to

Meeting our contractual obligations or rights

- managing payments between us
- meeting and performing our audit obligations
- recovering money owed to us or our group companies
- responding to requests made by you in relation to your information
- exercising our rights under our contract with you or applicable law

Legal and regulatory risk management

- detecting and preventing crime
- security and operations management
- managing risk for us, our group and our customers and users
- complying with our and our group's legal obligations
- keeping records accurate and up-to-date
- running our business in an efficient and proper way

Innovation and service improvement

- identifying new features, functionality and ways to meet customer and user needs
- studying how customers and users use our websites, apps and services
- creating anonymous reports and statistics
- creating anonymous data sets
- using Threat Data to improve, update and modify the service (including any block/allow lists, threat analysis, reports and records)

If you subscribe to our Prevent service, we do not use analysis of your behaviour (or, you are a business, your users' behaviour) to provide insight to other organisations and users (this is sometimes called 'cross-tenant insights')

Marketing and promotion

- enabling you to participate in competitions and promotions
- developing and carrying out marketing activities

How we process personal data lawfully

This table shows the main basis we rely on to process personal data. Sometimes there may be a secondary basis for the same type of processing (like keeping a financial transaction and then sharing it with authorities). If we share personal data, we only do so after careful consideration of whether it is necessary and lawful to do so. We will only share information where we have a contract with the receiving party which requires them to keep the information just as secure as if we store it, or where we are legally required to make the disclosure.

Action	Lawful Basis	Description / examples
Managing our relationship with you and/or your organisation	Contract, Legitimate Interest, Consent, Legal Obligation	Respond to your enquiries; pro-actively and re-actively manage your relationship with us; contact you; respond to your support calls and complaints; track engagement; notify you and any relevant regulator where we are legally or contractually required to do so.
Delivering our services	Contract	Providing you with access to the services you subscribe to; provide guidance; ensure our services are functioning properly; alert you to updates to your services.
Use of sub-processors	Contract, legitimate interest	Using cloud infrastructure to deliver our services
Meeting our contractual obligations or rights	Legal obligation, Contract	Sending and receiving of payments; recover money owed to us.
Exercising our contractual rights	Legitimate Interest, Legal Obligation	Exercising or enforcing our rights under our agreement with you
Legal and regulatory risk management	Legitimate Interest, Legal Obligation	Managing regulatory risk
Detect and prevent crime or breach of compliance obligations	Legitimate interest	Enabling us to detect and report criminal activity
Responding to Law Enforcement and obeying our legal obligations	Legitimate Interest, Legal Obligation	Assisting legal authorities where required or responding to legal or regulatory requests
Innovation and service improvement	Legitimate interest	Identifying new features, functionality and ways to meet customer needs; testing and releasing new features and functionality; creating anonymous reports and statistics
Marketing and promotion	Legitimate interest, Consent	Promote and grow our business; creating anonymous reports and statistics; enabling you to participate in promotions
System Messages	Legitimate Interest	Notification of business updates and renewals
Creating anonymous reports and statistics	Contract, Legitimate Interest	Showing a count of dangerous emails an organisation receives.
Carry out audits	Legitimate Interest, Legal Obligation	Evidence effective security processes and procedures

How we use automated decision-making

Some of our services may make use of machine learning. These services always involve some kind of meaningful human interaction during the processing activity meaning that if a particular email interaction, alert, or action is carried out, it has been done so by confirmation of a person. That person

may be yourself or a member your organisation's administrative or security teams. Where we have verified a particular message or action is malicious (such as a malware/ransomware email), then it may be automatically blocked. In these scenarios an administrator can always unblock any potential 'false-positive' restriction.

Who we may share your personal data with

Sub-Processors

You can find details on our Sub-Processors here. These third-parties provide key services to us that enable us to deliver our services to you or to run our own business operations. They are only authorised to use your personal data where this is necessary to provide the services to us that we request from them, and we have contracts in place with them that require they to comply with applicable law.

Examples of where they are involved include where they provide:

- hosting platforms (such as Microsoft Azure and Amazon Web Services) which we use to host our services
- Customer relationship management platforms
- Ticketing, online chat, out-of-hours support calls and other support service platforms that we use to provide our support services to you
- Multi-factor authentication services
- Mail relay delivery services
- Webinar, conference calls and remote access services
- Digital marketing platforms used to send out marketing communications
- Online editors (such as Microsoft Office Online) embedded in some of our products

Where personal data is transferred outside of the country or region that you are located in, we will ensure that it is subject to appropriate legal and technical safeguards as required by local law.

Law enforcement requests

We reserve the right to disclose personal data to comply with laws and legal or regulatory demands which apply to us, our group or our services. You can find out more on our approach here.

Online purchases

If you purchase a paid-for subscription to our services through our website, then limited personal data about you and your purchase will be shared with relevant payment service providers. Personal data may be used by those providers in accordance with their own privacy policies and terms to complete your purchase, manage your relationship and any future renewal, and to comply with applicable law.

Transfer of rights

We and our group companies reserve the right to transfer obligations, rights and permissions to any organisation to which we or they may transfer business or assets. This includes if a third-party is exploring investing in or purchasing us (or a relevant part of our group or assets).

Other important things to know

Privacy Shield

We participate in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and have self-certified to the U.S. Department of Commerce our adherence to the Privacy Shield Principles for all personal information received from countries in the European Economic Area, Switzerland, and the United Kingdom in reliance on the Privacy Shield. To learn more about Privacy Shield, visit the Privacy Shield website at www.privacyshield.gov/list. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall apply where it enables stronger protections.

Under Privacy Shield, we are responsible for the processing of personal information we receive and subsequently transfer to a third party acting for or on our behalf. We are liable for ensuring that the third parties we engage support our Privacy Shield commitments. The U.S. Federal Trade Commission has regulatory enforcement authority over our processing of personal information received or transferred pursuant to Privacy Shield. We commit to cooperate and comply with the advice of the regulatory authorities to whom you may raise a concern about our processing of personal information about you pursuant to Privacy Shield, including to the panel established by the EU authorities and the Swiss FDPIC. This is provided at no cost to you.

If you do not feel that we have resolved your complaint or concern satisfactorily you can contact our U.S. based third-party dispute provider (free or charge) at https://https://www.privacytrust.com/drs/open. Under certain conditions, more fully described on the Privacy Shield website, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

Complaints

If you have a complaint relating to our services you can raise it by emailing us or by calling +1-800-732-0746 (if you are in North America) or +44 (0) 20 3973 1333 (for anywhere else). Please note calls may be recorded and/or monitored for quality assurance and compliance purposes. Call recordings are stored in the United Kingdom and the United States.

If your complaint relates specifically to the processing of your personal information, please email us here.

You may also have the right to make a complaint at any time to a Supervisory Authority (such as the Information Commissioner's Office (ICO) in the UK). We would, however, appreciate the chance to deal with your concerns before you approach a regulator so please contact us in the first instance.

You can find our detailed Complaints Policy at www.egress.com/legal.

Changes to this policy

We may change this policy from time to time. You should check our website periodically to make sure that you have read our most up-to-date. When we do make changes, we will change the date at the top of this document.

About us

We are Egress Software Technologies Limited, for and on behalf of ourself and our group of companies. You can find out more details about us at www.egress.com/about and you can contact us at info@egress.com. When contacting us we strongly recommend you do not email us confidential or personal information. If you do, it is at your own risk although the terms of this policy will apply to our use of that information.

EU Representative

Egress Software Technologies Limited – Netherlands Branch (Herengracht 420, 1017 BZ, Amsterdam, The Netherlands. Registered number 74110462) is our EU representative for the purposes of Article 27 of the General Data Protection Regulation EU 2016/679.