POLICY ON DATA PROTECTION & PRIVACY STANDARDS ("POLICY")

Policy Overview:

1. **This Policy sets out how Marston's PLC and our group companies ("we", "our", "us", "the Company") handle the Personal Data belonging to our customers, suppliers, tenants, employees, workers and other third parties; whether past or present. Some key terms in this Policy are in capital letters, and to help you understand them, each term is defined in the glossary attached to this Policy.**

2. **This Policy applies to all Company personnel, including employees, workers contractors, consultants and directors ("you", "your"). During the course of your association with the Company, we will Process Personal Data about you (including Sensitive Personal Data) and this Policy sets out our obligations, and your rights, in relation to your Personal Data.**

3. **This Policy also explains your obligations, and what we expect from you, when processing any Personal Data on our behalf as part of your job duties. You must read, understand and comply with this Policy and undertake training as required. Your compliance with this Policy is mandatory and any breach may result in disciplinary action.**

4. **Protecting the confidentiality and integrity of Personal Data is a fundamental obligation of the Company. The proper and lawful treatment of Personal Data will help maintain confidence in the Company and help us ensure successful business operations. The Company is exposed to potential fines of up to 4% of total annual turnover for failure to comply with the Data Protection Legislation.**

5. **The Data Protection Officer is responsible for overseeing this Policy, and related policies and guidelines. The appointed Data Protection Officer at this time is Jonathan Moore, Corporate Risk Director, who can be contacted at DataSecurityInformation@Marstons.co.uk.**

6. **The Data Security Analyst is responsible for dealing with day to day Data Protection matters and any questions about the operation of this Policy, the Data Protection Legislation or any concerns that this Policy is not being followed, should be forwarded to them. In particular, you must always contact the Data Security Analyst if: you become aware of or suspect a Data Breach (see section 7), to update the Corporate Data Map (see section 12) and when a DPIA is required (see section 10).**

7. **This Policy is an internal document and cannot be shared with third parties, without the consent of the Data Security Analyst.**

1 DATA PROTECTION PRINCIPLES

1.1 The Company adheres to the data protection principles relating to Processing of Personal Data set out in the Data Protection Legislation which requires Personal Data to be:

a) Processed **lawfully, fairly** and in a **transparent** manner (*see section 2*);
b) Collected only for specified, explicit and **legitimate purposes** (*see section 3*);
c) Adequate, relevant and **limited to what is necessary** for the Processing (*see section 4*);
d) **Accurate** and where necessary kept up to date (*see section 5*);
e) Not kept in a form which permits identification of Data Subjects **for longer than is necessary** (*see section 4*);
f) Processed in a manner that ensures its security using **appropriate technical and organisational measures** to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (*see section 6*); and

1.2 The Company is responsible for, and must be able to demonstrate compliance with, the above

data protection principles. For further information, *see section 10* of this Policy which deals with how the Company ensures accountability.

2 LAWFUL, FAIR & TRANSPARENT

Lawfulness and Fairness –

2.1 Personal data must be processed **lawfully, fairly and in a transparent manner**. In accordance with the Data Protection Legislation, you may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting a Data Subject.

2.2 The Data Protection Legislation allows Processing for specific purposes, which are set out below:

a) the Data Subject has given their **Consent** (*see section 2.4*);
b) the Processing is **necessary for the performance of a contract** with the Data Subject or is necessary preparation for forming a contract with the Data Subject;
c) to meet our **legal obligations**;
d) to exercise official authority as a public body or to carry outa specific task in the public interest whereby it is mandated by law;
e) to protect the Data Subject's vital interests; or
f) to pursue our, the Data Subjects' or a third parties' **legitimate interests**, provided those interests are not overridden by the fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable privacy notice.

2.3 The lawful basis being relied on for each Processing activity must be identified and documented, before the processing begins. If you are unsure of the lawful basis which you are relying on to process Personal Data, please contact the Data Security Analyst, who will also document the decision.

Consent -

2.4 As we have seen, a Data Controller (in our case, the Company) must only process Personal Data on the basis of one or more of the lawful bases set out in the Data Protection Legislation, which include Consent.

2.5 A Data Subject consents to the Processing of their Personal Data if they indicate agreement clearly either by a **statement or positive action** to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

2.6 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented. Consent does not last indefinitely and as such should also be refreshed at appropriate intervals if there is continual processing for an extended period of time. If you are unsure of the nature of the Consent which you are relying on to process Personal Data, please contact the Data Security Analyst.

HINTS & TIPS

No matter what form marketing communications take, they should allow the recipient to opt out of receiving further marketing communications from the Company, such as an 'unsubscribe' link in an email. If any customer or business contact states that he or she does not wish to receive any (or particular) marketing information from us, we should comply promptly with this instruction. Not only would we breach Data Protection Legislation if we failed to do so, it makes no business sense to continue to send marketing material to a contact who no longer wishes to hear from us and it could damage our reputation with that customer or business contact.

2.7 Unless we can rely on another legal basis for Processing, explicit Consent (a very clear and specific statement) is usually required for Processing Sensitive Personal Data and any automated decision-making (for example, a form of automated Processing to evaluate, analyse or predict a Data Subject's economic situation, personal preferences, behaviour, or location, such as profiling). Usually we will be relying on another legal basis to Process most types of Sensitive Data, but where consent is required, you must issue a Privacy Notice to the Data Subject to capture explicit Consent and keep records of all Consents (*see section 12*). If you need to rely on or capture Consent, or draft a Privacy Notice, please contact the Data Security Analyst.

Transparency (Privacy Notices) -

2.8 The Data Protection Legislation requires all Data Controllers to provide detailed, specific information to Data Subjects in the form of Privacy Notices. Privacy Notices must be **concise, transparent, intelligible, easily accessible, and in clear and plain language** so that a Data Subject can easily understand them.

2.9 Whenever we collect Personal Data directly from Data Subjects, including for recruitment or employment purposes, we must provide the Data Subject with all the information required by the Data Protection Legislation including the identity of the Data Controller and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice. Privacy Notices must be presented when the Data Subject first provides the Personal Data.

2.10 Privacy Notices, wherever located, must not be used or amended without the approval of the Data Security Analyst.

3 PURPOSE LIMITATION

3.1 Personal Data must be collected only for **specified, explicit and legitimate purposes**.

3.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained, unless you have informed the Data Subject and they have provided their Consent, where necessary.

4 DATA MINIMISATION & STORAGE LIMITATION

4.1 Personal Data must be **adequate, relevant and limited** to what is necessary in relation to the purposes for which it is processed. Personal Data must not be kept for longer than is necessary for the purposes for which the data is processed

4.2 You may only Process Personal Data when performing your job duties, and you must only collect Personal Data that is relevant to the job at hand. Do not collect excessive data and ensure any Personal Data collected is adequate and relevant for the intended purposes. You may not Process Personal Data for any reason unrelated to your job duties.

4.3 You must not keep Personal Data in a form which permits the identification of the Data Subject

for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

4.4 The Company maintains retention and classification policies and procedures to ensure Personal Data is kept safe and deleted or destroyed as soon as possible after the purpose for collecting it has come to an end. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted, destroyed or (where applicable) anonymised in accordance with the Company's data retention and classification policy, which can be accessed on the Marston's Hub. This includes requiring third parties to delete such data where applicable.

4.5 If you require guidance on how to safely delete or anonymise personal data, please contact the IT Service Desk (Extension: 1500 Email: itservicedesk@marstons.co.uk).

4.6 You must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

5 ACCURACY

5.1 Personal Data must be **accurate and, where necessary, kept up to date**. It must be corrected or deleted without delay when inaccurate.

5.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

6 SECURITY INTEGRITY AND CONFIDENTIALITY

Protecting Personal Data –

6.1 Personal Data must be kept safe and secure by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

6.2 We will develop, implement and maintain safeguards appropriate to our size, scope of business and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

6.3 You are also responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

6.4 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures. Please contact the Data Security Analyst for further information in relation to our policies and procedures in relation to third parties, including checking the technical and operational measures implemented by those third parties to maintain the security of Personal Data.

6.5 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data you Process, as follows:

HINTS & TIPS

Any Personal Data that needs to be transmitted externally (such as to a Data Subject or a service provider) must only be sent if a secure network, or comparable arrangements such as encryption or password protection, are in place. Please contact the IT Service Desk to help you determine the safest method of transfer in all cases.

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular you should consider that the caller put their request in writing if you are not sure about their identity.

Remember it is only permissible to disclose personal information relating to a Data Subject, to that Data Subject and not, for example, to a member of their family, unless we have their express written consent or we are required to disclose the information by law.

a) **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it;

b) **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed;

c) **Availability** means that authorised users are able to access the Personal Data when they need it for authorised purposes; and

d) You must comply with all applicable aspects of our Group Information Technology Policy & Social Media Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement from time to time.

7 REPORTING A DATA BREACH

7.1 The Data Protection Legislation requires us to notify a Data Breach to the ICO and, in certain instances, the Data Subject. A data breach is more than just the loss of Personal Data, it includes a breach of security leading to destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

7.2 We have put in place incident response procedures to deal with any suspected Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

7.3 If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself. Instead, **immediately** contact the Data Security Analyst or any member of the Data Security Committee (current members can be located via the document titled “Data Security Committee Members and Contacts” on the Hub) or another member of the Cosec, Legal & Risk Team, and they will follow the incident response plan.

7.4 We must preserve all evidence relating to the potential Data Breach to help minimize harm to the Data Subjects, therefore please do not share any details relating to the Data Breach with any colleagues or third parties, unless you are permitted to do so.

8 TRANSFER LIMITATION

8.1 The Data Protection Legislation restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the Data Protection Legislation is not undermined.

8.2 You may only transfer Personal Data outside the UK with the consent of the Data Security Analyst and only then if one of the following conditions applies:

a) the UK Government has issued a decision confirming that the country to which we

transfer the Personal Data ensures an adequate level of protection;

b) appropriate safeguards are in place such as Binding Corporate Rules (BCRs), Standard Contractual Clauses, applicable Codes of Conduct or Certification Mechanisms;

c) the Data Subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in The Data Protection Legislation.

8.3 Following the UK's exit from the EU, the UK now operates on the basis of the UK General Data Protection Regulation and the Data Protection Act 2018. The European Commission have granted the UK an adequacy decision which is set to be in place until June 2025, however it can be revoked at an earlier date. The UK Government has likewise approved transfers of personal data from the UK to EEA countries. The UK Government is also working with other countries that hold an adequacy decision from the European Commission, to assess whether a formal decision can be put in place to enable transfers of data. For guidance on any such matters please speak to the Data Security Analyst.

9 DATA SUBJECT'S RIGHTS AND REQUESTS –

9.1 Data Subjects (including you as an employee of the Company) have rights when it comes to how we handle their Personal Data. These include (but are not limited) the right to:

a) withdraw Consent to Processing;

b) receive certain information about the Data Controller's Processing activities;

c) request access to their Personal Data that we hold, known as a subject access request or "SAR";

d) rectify inaccurate data or to complete incomplete data;

HINTS & TIPS

The time period for dealing with a Subject Access Request is currently one calendar month and we cannot charge a fee to deal with the request.

The Company has a Subject Access Request form (available from the Hub)which we invite Data Subjects to complete in the event they wish to make a SAR so that we may verify their identity and gather sufficient information to enable us to comply within the timeframe specified by the Data Protection Legislation. It is important to note the use of that form to provide the relevant information is not obligatory and a request can be made verbally if required.

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected. This is also known as "the right to be forgotten";

f) prevent our use of their Personal Data for a period of time, for specific reasons;

g) request movement of their personal data from one IT environment to another. This is "the right to data portability";

h) object to and challenge Processing decisions in certain circumstances;

i) not be subject to automated decision making and profiling, unless under specific circumstances; and

9.2 If you receive, or wish to make, a request, you should forward it to the Data Security Analyst immediately, as in most cases, we are obliged to respond to such requests within one calendar month of receipt. The Data Security Analyst is responsible for handling the request and ensuring resolution, except only in the cases of internal employment requests in which the relevant HR team will take the lead.

9.3 The identity of an individual requesting any data under any of the rights listed above must be

verified. Do not allow third parties, even the Police, to persuade you into disclosing Personal Data without proper authorisation. Please refer all requests to the Data Security Analyst.

10 ACCOUNTABILITY

10.1 The Data Controller must implement appropriate technical and organisational measures to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

10.2 The Company must have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including (but not limited to):

a) **Implementing Privacy by Design when Processing Personal Data –** The Company (and you, if it forms part of your duties) must assess what Privacy by Design measures can be implemented on all systems or processes that Process Personal Data by taking into account: the nature, scope, context and purposes of Processing, the cost of implementation and the risks to the rights and freedoms of Data Subjects;

b) **Completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects** – A DPIA is mandatory when implementing major system or business change programs involving the Processing of Personal Data including (but not limited to) the use of new, or changing existing, technologies (such as systems or processes), automated processing including profiling; large scale Processing of Sensitive Data; and large scale, systematic monitoring of a publicly accessible area. A DPIA must be carried out under the supervision of the Data Security Analyst;

c) **Integrating data protection into internal documents including this Policy and Privacy Notices** - You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data;

d) **Training Company personnel on the Data Protection Legislation and related policies** - If you Process Personal Data as part of your duties, you are required to undertake a mandatory eLearning Module and (if you are a line manager) ensure your team undergo the mandatory training too. If you have not received the instructions to access the eLearning Module, or if you are aware that members of your team have not, please contact the Data Security Analyst; and

e) **Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort**.

11 HOW WE PROCESS YOUR PERSONAL DATA

11.1 We value the privacy and rights of our employees. Whilst many of the principles in this Policy relate to Personal Data belonging to our employees, as well as other Data Subjects connected to the Company, this part of the Policy specifically outlines our practices in relation to the collection and use of information about you.

11.2 Good practice and the efficient running of the Company require us to hold Personal Data about you, including Sensitive Personal Data, such as information on your health, racial or ethnic origin or marital status. We obtain personal information about you from several sources; from the application form you submitted when you applied to join the Company to any other details you subsequently provide to us. We will also keep records of, for example, your absence history, your performance reviews (PCDR) and any actions or decisions taken as a result of applying any of our policies.

11.3 The Company operates an employee privacy policy which goes into further detail around the processing of your data as an employee. This can be found on the Hub or you can request a copy from the Data Security Analyst.

Use of data without your knowledge

11.4 The Company is ultimately responsible for all business communications but, so far as

possible, your privacy will be respected. We may monitor your communications for specific reasons which include: ensuring that our procedures & policies are adhered to; complying with our legal obligations; and preventing or detecting unauthorised use of our IT systems or criminal activities. Further information can be found in our Group Information Technology Policy & Social Media Policy. Such monitoring will take place in accordance with the Act and related regulations, such as the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

11.5 Please be aware that under the Data Protection Legislation, we can share your Personal Data without your knowledge for the purposes of: the prevention or detection of crime; the apprehension or prosecution of offenders; a rule of law or by the order of the court; or the assessment or collection of tax or duty.

11.6 We will make every effort to ensure that the Personal Data held about you is accurate and, where necessary, kept up to date. It is your responsibility to ensure that the information contained in our HR database is accurate and kept up to date. You can do this by informing us promptly of any changes to your details, such as a change of address or updating your own detail on our Employee Self-Service system. In the absence of evidence to the contrary we shall assume that the information you provide is accurate. If there is any reasonable doubt as to the accuracy of the Personal Data, we shall contact you to confirm the information. Should you inform us, or we otherwise become aware, of any inaccuracies in the information, they shall be rectified promptly.

11.7 You have the right to request access to, or information about, your Personal Data in relation to your employment as set out in section 9 of this Policy.

12 RECORD KEEPING

12.1 The Data Protection Legislation requires us to keep full and accurate records of all our data Processing activities.

12.2 The Data Security Analyst has undertaken and is responsible for maintaining a Corporate Data Map and associated accountability documentation. To ensure that all Company Processing activities are included on these documents, you must report all new activities or processes involving the processing and storage of Personal Data, including changes to existing processes and records of Data Subjects' Consents to the Data Security Analyst and attend all meetings requested by the Data Security Analyst for this purpose.

13 DIRECT MARKETING

13.1 We are subject to certain rules and privacy laws when marketing to our customers. For example, a **Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or phone calls).** The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

13.2 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

13.3 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

HINTS & TIPS

Different rules apply to marketing to individuals (such as customers in our pubs) and in 'business to business' context (such as corporate customers, like free trade accounts or wholesalers):

- **You should not send marketing material to an individual through electronic channels without first obtaining their consent in accordance with this Policy.**
- **In 'business to business' contexts, there is no legal requirement to obtain an indication of consent to carry out electronic marketing to a "business contact", provided that it is carried out in a business context, and we are not marketing to them in a personal capacity. Therefore, sending an email to a business contact's business email address (such as joe.bloggs@UKcompany.com), advertising a product or service we can offer the UK company, would fall into the 'business context,' however, sending an email to Joe Bloggs' personal email address to advertise Company products and services would not. The same rules apply in the context of marketing telephone calls.**

14 SHARING PERSONAL DATA

14.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

14.2 You may only share the Personal Data we hold with another colleague if they have a job-related need to know the information.

14.3 You may only share the Personal Data we hold with third parties, such as marketing agencies or other suppliers if:

a) they have a need to know the information for the purposes of providing the services;
b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and
d) a fully executed written contract that contains Data Protection Legislation approved third party clauses, has been obtained.

Please speak to the Data Security Analyst for help with the appropriate documentation and undertaking the required checks in relation to the third parties' security measures. The legal team can also support you with ensuring the contract complies with the Data Protection Legislation.

14.4 Given the scope of modern technology, it is common practice that Personal Data, including images or videos are uploaded to Social Media platforms from time to time. It is important we consider the implications this may have on a Data Subject, particularly if they are a child or a vulnerable person. Where possible (at organised events and similar) a consent form should be sought from the Data Subject or responsible parent or guardian to take photos or videos and reproduce them in a public format. Signage should also be available on the day to inform the Data Subject or responsible person of potential photography/recording and reproduction. A standardised form exists for this purpose and can be found on the Hub. Head Office teams should contact the Legal department in order to attain a tailored form specific to their project. Please see the Social Media Policy for further information.

15 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time so please check back regularly to obtain the latest copy of this Policy. The most recent version of the Policy will always be available on the on the Hub.

Where collective bargaining arrangements exist we will consult elected Employee Representatives regarding such changes.

See footer for version control details

Next review: July 2022

Reviewed by:
G Checkley (Data Security Analyst) – July 2021

Approved by:
J Moore (Data Protection Officer) – July 2021

GLOSSARY

"Consent"	means agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by

	which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
"Corporate Data Map"	means a map (together with appropriate data flows) of all Personal Data Processed by the Company including the nature of the Personal Data Processed, the scope of the Processing activities, any third-party recipients of the Personal Data, storage location of the Personal Data and where relevant, a description of the security measures in place.
"Criminal Offence Data"	means data relating to criminal allegations, proceedings or convictions, and any related security measures. This data would have previously been sensitive personal data under previous legislation but is now afforded more specific and enhanced protection.
"Data Breach"	means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Company or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Data Breach.
"Data Controller"	means the person or organisation that determines when, why and how to process Personal Data and is responsible for establishing practices and policies in line with the Data Protection Legislation. The Company is the Data Controller of all Personal Data relating to our Company personnel and Personal Data used in our business for our own commercial purposes, such as customer, tenant or employee data.
"Data Protection Legislation"	means the UK General Data Protection Regulation, the Data Protection Act 2018, (to the extent applicable to the business) the General Data Protection Regulation (*(EU) 2016/679*) and any other legislation amending, enacting or updating such laws from time to time.
"Data Security Analyst"	means the person voluntarily appointed by the Company with day-to-day responsibility for data protection compliance.
"Data Subject"	means a living, identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and have legal rights regarding their Personal Data.
"DPIA"	or Data Privacy Impact Assessment mean tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the Processing of Personal Data and always under the supervision of the Data Security Analyst.

"EEA"	the 27 countries in the EU, and Iceland, Liechtenstein and Norway.
"Privacy Notices"	mean notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.
"ICO"	means the Information Commissioner's Office, an independent body who regulates and oversees data protection in the United Kingdom. The ICO can be contacted here https://ico.org.uk/global/contact-us/.
"Personal Data"	means any information identifying a Data Subject, or information relating to a Data Subject which means we can identify the Data Subject when we combine it with other information we have access to, and includes Sensitive Personal Data, but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth), an opinion about that person's actions or behaviour (for example, an appraisal) or (generally) an image of that person.
"Processing" or "Process"	means any activity that involves the use of Personal Data. It includes obtaining, recording, hosting or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
"Special Category Data"	means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation and biometric or genetic data..