General Data Protection Policy

1. Introduction

GlobalBlock Limited ("GlobalBlock") respects the privacy of all individuals and takes very seriously its responsibilities under the General Data Protection Regulation (2016). This policy is designed to ensure that all information held on individuals is properly handled in all cases.

The firm's reputation is dependent upon the trust of its clients and staff. Adherence with this policy will ensure the company's high reputation is protected.

2. Scope

This policy applies to all staff working within GlobalBlock (including directors, employees, agency workers, contractors, consultants and temporary staff) who may process personal data about individuals the firm has a relationship with or employees.

The policy applies to all data that GlobalBlock holds relating to identifiable individuals, even if that information technically falls outside the data protection law. This can include individuals':

- Name
- Postal address
- Email address
- Telephone number
- IP address
- Mobile phone device IDs
- Trading activity
- Financial information
- And any other specific personal information relating to the individuals such as the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Compliance with this policy is mandatory.

Personal data is defined very widely and is any data from which a living individual can be identified either from the information alone, or with other information which is in (or likely to come into) the possession of the UK operating company. Examples of personal data include names, addresses, photographs, CCTV images of individuals, salary/job titles, IP address or opinions which allow individuals to be identified. Personal data also includes "sensitive personal data" – this is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life or criminal offences/proceedings.

3. Background to the General Data Protection Regulation (GDPR)

The European Parliament adopted the GDPR in April 2016, replacing the Data Protection Act (1998). The purpose of GDPR is to provide a set of standardised data protection laws across all of the

member countries. This should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where it is located. It seeks to give individuals more control over how organisations use their data, with the long-term aim of legally safeguarding data security rights in the digitalised world.

4. Definitions

"Individuals" could be any living person – for example, employees, agency staff, customers, contractors, suppliers and job applicants.

"Processing" means any operation or setoff operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, or combination, restriction, erasure or destruction

"Personal Data" means any information relating to an identified or identifiable natural person (data subject) is one who can be identified, directly or indirectly, in particular by reference to an identifies such as a name, an identification, number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

"Data Subject" means the identified or identifiable natural person to which the data refers

"Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State Law, the controller or the specific criteria for its nomination may be provided for by Union or Member State Law

"Consent" of the data subject means any freely given, specific, informed an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relation to him or her

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

"Personal data breach" means a breach of security leading to accidental or unlawful destruction, loss, altercation, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

5. Governance

The Board is responsible for the oversight of data protection. The compliance department will be responsible for data protection matters and applying risk based systems and controls to ensure the policy is being complied with. Queries relating to data protection matters should be referred to the Compliance department.

6. Consent

GlobalBlock will obtain personal data only by lawful and fair means, and where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, GlobalBlock is committed to seeking such consent.

GlobalBlock will ensure that their system includes provisions for:

- Determining what disclosures should be made to obtain valid consent
- Ensuring the requires for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language
- Ensuring that consent is freely given (i.e. is not based on a contract that is conditional to the processing of personal data that is unnecessary for the performance of that contract)
- Documenting the date, method and content of the disclosure made, as well as the validity, scope and volition of the consents given
- Providing a simple method for a data subject to withdraw their consent at any time

7. Data Processing

GlobalBlock uses the personal data of its clients for the following broad purposes:

- To provide services to our clients
- The onboarding of new clients and employees
- The general running and business administration of GlobalBlock
- The ongoing administration and management of our client services and relationship management

The use of the data subject's information should always be considered from their perspective and whether the use will be within their expectation or if they are likely to object. For example, it would clearly be within our client's expectations that their detail will be used by GlobalBlock to respond to a request from the client about the products and services on offer. However, it will not be within their reasonable expectations that GlobalBlock would then provide their details to the third parties for marketing purposes.

GlobalBlock will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, GlobalBlock will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in data controller
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party (for example, due diligence checks when onboarding new clients or employees). However, this does not apply where interests are overridden by the interests of fundamental rights and freedoms of the data subject, in particular where the data subject is a child.

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When deciding as to the compatibility of the new reason for processing, guidance and approval must be obtained from ICO before any such processing may commence.

8. Principles relating to the processing of Personal Data (Article 5 GDPR)

1. Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, GlobalBlock must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for the purposes specified in applicable regulation..
2. Purpose Limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means GlobalBlock must specify what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.
3. Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means GlobalBlock must not store any personal data beyond what is strictly required.
4. Accuracy	Personal data shall be accurate and, where necessary, kept up to date. This means GlobalBlock must be able to identify and address out-of- date, incorrect and redundant personal data.
5. Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for

	which the personal data are processed. This means that GlobalBlock, wherever possible, must store personal data in a way that limits or prevents identification of the data subject.
6. Integrity and Confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. GlobalBlock must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.
7. Accountability	The controller shall be responsible for, and be able to demonstrate compliance with GDPR. This means GlobalBlock must demonstrate the six Data Protection Principles (outlined above) are met for all personal data which it is responsible. .

9. Individuals' rights

Right to be informed (Article 13 and 14)

Individuals have the right to be informed about the collection and use of their personal data and this is a key transparency requirement under GDPR.

GlobalBlock is required to provide 'privacy information' to individuals at the time we collect personal data from them. In brief the 'privacy information' should include:

- GlobalBlock's purposes for processing their personal data
- GlobalBlock's retention periods for that personal data
- Who the information will be shared with

More details on this information is included in Appendix A.

The information must be:

- Concise
- Transparent
- Intelligible
- Easily accessible
- In clear and plain language

GlobalBlock ensures that clients are kept informed through privacy notices which have been sent by email.

In the case of GlobalBlock obtaining personal data from a source other than the individual it relates to, GlobalBlock will provide the individual with privacy information:

- Within a reasonable a period of obtaining the personal data and no later than one month

- If the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- If disclosure to someone else is envisages, at the latest, when the data is disclosed

When obtaining personal data from other sources, GlobalBlock does not need to provide individuals with privacy information if:

- The individual already has the information
- Providing the information to the individual would be impossible
- Providing the information to the individual would involve a disproportionate effort
- Providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing
- GlobalBlock is required by law to obtain or disclose the personal data; or
- GlobalBlock is subject to an obligation of professional secrecy regulated by law that covers the personal data

GlobalBlock will regularly review, and where necessary, update your privacy information.

Right to access (Article 15)

All individuals who are the subject of personal data held by GlobalBlock are entitled to the following information:

- Confirmation that their data is being processes
- Access to their personal data
- The purpose of the processing
- The categorises of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible the criteria used to determine that period
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object such processing
- The right to lodge a complaint with a supervisory authority
- Where the personal data are not collected from the data subject, any available information as to their source
- The existence of automated decision-making including profiling, meaningful information about the logic involved, as well as the envisaged consequences of such processing for the data subject

Requests from individuals are made via email, addressed GlobalBlock. GlobalBlock can supply a standard request form, although individuals do not have to use this. GlobalBlock will verify the identity of anyone making a subject access request before providing the information.

Individuals will not be charged a fee for this GlobalBlock will aim to respond within 14 days but no longer than a month except in cases of particularly complex requests this may be extended to a further two month. However, GlobalBlock must notify the individual of this within a month of receipt of the request, providing our reasons without delay. GlobalBlock also has the right to refuse to respond to a request in which case we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and the latest within one month.

Right to Erasure (Article 17)

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as the 'right to be forgotten'. This can be made by the individual verbally or in writing.

Individuals will have the right to have their personal data erased if:

- The personal data is no longer necessary for the purpose which GlobalBlock originally collected or processed it for
- GlobalBlock is relying on consent as its lawful basis for holding the data, and the individual withdraws their consent
- GlobalBlock is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data and there is not overriding legitimate interest to continue this processing
- GlobalBlock is processing the personal for direct marketing purposes and the individual objects to that processing
- GlobalBlock has processed the personal data unlawfully (in breach of Principle 1)
- GlobalBlock have to do it to comply with a legal obligation

There are two circumstances in which GlobalBlock will tell other organisations about the erase of personal data:

- The personal data has been disclosed to others
- The personal data has been made public in an online environment

The right to erasure will not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation
- For the performance of a task carried out in the public interest or in the exercise of official authority
- For achieving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- For the establishment, exercise or defence of legal claims

GlobalBlock can refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. In these cases, we can request a "reasonable fee" (in which case we will contact the individual promptly and inform them) to deal with the request or refuse to deal with the request. If a request is refused, GlobalBlock will inform the individual without undue delay and within one month of receipt of the request. We will inform the individual about the reasons we are not taking the action, their right to make a complaint

to the ICO or another supervisory authority and their ability to seek to enforce this right through a judicial remedy.

Right to Rectification (Article 16)

Individuals will have the right to have inaccurate personal data rectified and this can be made verbally or in writing. Although GlobalBlock may have already taken steps to ensure that the personal data was accurate when they obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

If the GlobalBlock receive a request for rectification, they will take reasonable steps to satisfy themselves that the data is accurate and to rectify the data if necessary. This should take into account the arguments and evidence provided by the data subjects. The GDPR does not give a definition of the term accuracy. However, the Data Protection Bill states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

As a matter of good practice, GlobalBlock will restricting the processing of any personal data in questions whilst verifying its accuracy.

GlobalBlock has one month to respond to a request and will let the individual know if they are satisfied the personal data is accurate, and tell them that they will be not be amending the data. They will then example their decision, inform them of their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce their rights through a judicial remedy.

GlobalBlock can refuse to comply with a request for rectification if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. In these cases, we can request a “reasonable fee” (in which case we will contact the individual promptly and inform them) to deal with the request or refuse to deal with the request. If a request is refused, GlobalBlock will inform the individual without undue delay and within one month of receipt of the request. We will inform the individual about the reasons we are not taking the action, their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce this right through a judicial remedy.

Right to Restrict Processing (Article 18)

Individuals have the right to request the restriction or suppression of their personal data and this can be requested verbally or in writing.

The right to restrict the processing of personal data can be done in the following circumstances:

- The individual contests the accuracy of their personal data and they are verifying the accuracy of the data
- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead
- GlobalBlock no longer needs the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim
- The individual has objected to us processing their data (under Article 21 of their Right to Object) and we consider whether out legitimate grounds override those of the individual

We will restrict the data by:

- Temporarily moving the data to another processing system
- Making the data unavailable to users
- Temporarily removing published data from a website (if we were to put it on a website)

Once the data restricted, GlobalBlock will not restrict it any wat except to store it unless:

- We obtain the individual's consent
- It is for the establishment, exercise or defence of legal claims
- It is for the protection of the rights of another person
- It is for reasons of important public interest

GlobalBlock will refuse based on the same reasons as refusing to rectification, access and erasure and the same information and time limits apply.

Right to Data Portability (Article 20)

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. This allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This will only apply when the individual has provided consent and this has been done by automated means.

GlobalBlock has the right to respond without undue delay, and within one month. This can be extended by two months where the request is complex or GlobalBlock receives many requests. GlobalBlock will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Right to Object (Article 21)

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of statistics and scientific/historical research (which would not apply to GlobalBlock)

GlobalBlock must stop processing the personal data unless:

- GlobalBlock can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Rights related to automated decision making including profiling (Article 22)

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling.

GlobalBlock will only carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- Necessary for entering into or performance of a contract between an organisation and the individual
- Authorised by law
- Based on the individual's explicit consent

The right to object must be stated in the privacy notice.

10. Data Protection Impact Assessment

GlobalBlock will do a Data Protection Impact Assessment (DPIA) before carrying out processing likely to result in high risk individuals' interests. This means that although the actual level or risk may not be assessed yet, GlobalBlock need to screen for factors which point to potential for a widespread or serious impact on individuals. In particular, GlobalBlock will be do a DPIA if they plan to:

- Use new technologies
- Use systematic and extensive profiling with significant effects
- Process special category or criminal offence data on a large scale
- Systematically monitor publicly accessible places on a large scale
- Profile individuals on a large scale
- Match data or combine datasets from different sources
- Collect personal data from a source other than the individual without providing them with a privacy notice

If the need arises, GlobalBlock will use this data template provided by the Information Commissioner Officer- https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

11. General Guidelines

Employees should keep all data secure, by taking sensible precautions and following guidelines set out by GlobalBlock. Personal data should not be disclosed to unauthorised parties, either within GlobalBlock or externally.

GlobalBlock operates a clear desk policy. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it. Computer screens should be locked when desks are left unattended.

Data that is usually stored electronically but has been printed out:

- Should be kept in a locked drawer of a filing cabinet.
- Should not be left where unauthorised people could see them e.g. on a printer.
- Should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- Data should only be stored on designated GlobalBlock drives and servers.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently and those backups should be tested regularly and should be subject to the very same security provisions as for live databases.
- All servers and computers containing data should be protected by approved security software and a firewall.

When personal data is accessed, used and shared, it can be exposed to the risks of loss, corruption or theft.

- Personal data should not be shared informally. As such personal data should always be transferred via GlobalBlock's secure networks and never be sent by email.
- If personal data is transferred electronically, the data must be encrypted before being transferred.
- Personal data should never be transferred outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data. GlobalBlock should be consulted if you need to transfer data outside of the EEA.

12. Breaches

Personal data breach means a breach of security leading to accidental or unlawful destruction, loss, altercation, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

All breaches of data security (such as the loss of personal data) will be reported the Compliance department. All staff will co-operate with the Compliance department in the investigation and management of the breach.

13. Penalties

Under GDPR, organisations in breach can be fined up to 4% annual global turnover of €20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g not have sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervisory authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors meaning 'clouds' will not be exempt from GDPR enforcement.

The two tiers of administrative fines that can be levied are:

1) Up to €10 million, or 2% annual global turnover
2) Up to €20 million, or 4% annual global turnover

14. Monitoring and Reporting

The Compliance department will oversee the appropriate reviews and audits to address the data protection risks identified. At least annually, or more frequently if required, this will be reported to the board on data protection compliance and risks.

15. Training

The compliance department will ensure that the level of knowledge on data protection is adequate and provide training where necessary.

16. Third Parties

GlobalBlock will satisfy itself that any third party it appoints to manage data on its behalf understands its responsibilities under the DPA. GlobalBlock will enter into a contract with the third party that requires it to act only on the instructions of the firm and requires it to comply with the obligations equivalent to those of GlobalBlock in respect of the security of personal data.

APPENDIX A

This table summarises the information that GlobalBlock must provide. What we will need to tell people differs slightly depending on whether we collect personal data from the individual it relates to or obtain it from another source.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

Document Control

Document name: Data Protection Policy

Effective from Date:

Version: 1.0

Owner:

Date of last amendment: