

# Data Protection Policy

## GDPR - External

**Prepared by: Compliance Department**

#### **DISCLAIMER**

*360Globalnet and associated companies do not assume any responsibility for incidental or consequential damages. This publication is provided on the basis that no warranty or representations (express or implied) are made concerning the contents of the publication. It is not intended that the contents of this publication form part of the terms of any agreements.*

*Any reference to 360Globalnet and associated companies' products, programming or services, shall not impose an obligation on the 360Group of companies to provide such products, programming or services to a particular person or at a particular location.*

*This publication may include inaccuracies or errors and should not be relied on without independent verification. Further, 360Globalnet or associated companies may alter this publication, produce a new edition or version of the publication, or modify, improve or change any products or programs described in this publication without prior notice.*

1.	Introduction .....	3
2.	The Data Protection Principles .....	3
3.	The Rights of Data Subjects .....	4
4.	Lawful, Fair, and Transparent Data Processing .....	4
5.	Specified, Explicit, and Legitimate Purposes .....	6
6.	Adequate, Relevant, and Limited Data Processing.....	6
7.	Accuracy of Data and Keeping Data Up to Date .....	6
8.	Data Retention.....	6
9.	Secure Processing .....	7
10.	Accountability and Record-Keeping .....	7
11.	Data Protection Impact Assessments.....	7
12.	Keeping Data Subjects Informed .....	8
13.	Data Subject Access.....	9
14.	Rectification of Personal Data .....	9
15.	Erasure of Personal Data .....	10
16.	Restriction of Personal Data Processing.....	10
17.	Data Portability.....	10
18.	Objections to Personal Data Processing.....	11
19.	Automated Decision-Making.....	11
20.	Profiling.....	12
21.	Personal Data Collected, Held and Processed.....	13
22.	Data Security – Transferring Personal Data and Communications .....	14
23.	Data Security – Storage .....	14
24.	Data Security – Disposal .....	15
25.	Data Security – Use of Personal Data .....	15
26.	Data Security – IT Security.....	16
27.	Organisational Measures.....	16
28.	Transferring Personal Data to a Country Outside the EEA.....	17
29.	Data Breach Notification .....	18
30.	Mutual Legal Assistance requests/Judicial Cooperation .....	19
31.	Implementation of Policy .....	20

## 1. Introduction

This Data Protection Policy (the “Policy”) sets out the principles and obligations of 360Globalnet Ltd, a company registered in England and Wales, company registration number 07127114, registered office Bourne House, 475 Godstone Road, Whyteleafe, Surrey, CR3 0BL (the “Company”) regarding data protection and the rights of clients, business contacts and employees (“data subjects”) in respect of their personal data under the General Data Protection Regulation ((EU) 2016/679) (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

## 2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

- 2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- 2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- 2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- 2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- 2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- 2.6 Processed in a manner that ensures appropriate security of the personal data,

including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

### 3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- 3.1 The right to be informed (Part 12).
- 3.2 The right of access (Part 13);
- 3.3 The right to rectification (Part 14);
- 3.4 The right to erasure (also known as the ‘right to be forgotten’) (Part 15);
- 3.5 The right to restrict processing (Part 16);
- 3.6 The right to data portability (Part 17);
- 3.7 The right to object (Part 18); and
- 3.8 Rights with respect to automated decision-making (Parts 19 and 20).

### 4. Lawful, Fair, and Transparent Data Processing

- 4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
  - 4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;
  - 4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
  - 4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;
  - 4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;
  - 4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
  - 4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- 4.2 If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity,

politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- 4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- 4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- 4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- 4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- 4.2.5 The processing relates to personal data which is clearly made public by the data subject;
- 4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- 4.2.7 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- 4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- 4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy);  
or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

## 5. Specified, Explicit, and Legitimate Purposes

- 5.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:
  - 5.1.1 Personal data collected directly from data subjects; and
  - 5.1.2 Personal data obtained from third parties including suppliers, clients and their customers
- 5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).
- 5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

## 6. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

## 7. Accuracy of Data and Keeping Data Up to Date

- 7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.
- 7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

## 8. Data Retention

- 8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- 8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

- 8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy and Addendum.

## 9. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

## 10. Accountability and Record-Keeping

- 10.1 The Company's Data Protection Officer is Lorraine Fiander, [lorraine.fiander@360globalnet.com](mailto:lorraine.fiander@360globalnet.com) or [dataprotection@360globalnet.com](mailto:dataprotection@360globalnet.com).
- 10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.
- 10.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- 10.3.1 The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
  - 10.3.2 The purposes for which the Company collects, holds, and processes personal data;
  - 10.3.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
  - 10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
  - 10.3.5 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy and Addendum); and
  - 10.3.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

## 11. Data Protection Impact Assessments

- 11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.
- 11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
- 11.2.1 The type(s) of personal data that will be collected, held, and processed;

- 11.2.2 The purpose(s) for which personal data is to be used;
- 11.2.3 The Company's objectives;
- 11.2.4 How personal data is to be used;
- 11.2.5 The parties (internal and/or external) who are to be consulted;
- 11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- 11.2.7 Risks posed to data subjects;
- 11.2.8 Risks posed both within and to the Company; and
- 11.2.9 Proposed measures to minimise and handle identified risks.

Data Protection Impact Assessment Forms can be found on your business repository or obtained from the Data Protection Officer.

## 12. Keeping Data Subjects Informed

- 12.1 The Company shall provide the information set out in Part 12.2 to every data subject:
  - 12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
  - 12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - a) if the personal data is used to communicate with the data subject, when the first communication is made; or
    - b) if the personal data is to be transferred to another party, before that transfer is made; or
    - c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
- 12.2 The following information shall be provided:
  - 12.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;
  - 12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
  - 12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
  - 12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
  - 12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;
  - 12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);



- 12.2.7 Details of data retention;
- 12.2.8 Details of the data subject's rights under the GDPR;
- 12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- 12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- 12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- 12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

### 13. Data Subject Access

- 13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
- 13.2 Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the Company's Data Protection Officer.
- 13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed within a month of receiving the SAR and explain why the extension is necessary.
- 13.4 All SARs received shall be handled by the Company's Data Protection Officer.
- 13.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

### 14. Rectification of Personal Data

- 14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
- 14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- 14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

## 15. Erasure of Personal Data

- 15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
  - 15.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
  - 15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
  - 15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
  - 15.1.4 The personal data has been processed unlawfully;
  - 15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.
- 15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- 15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## 16. Restriction of Personal Data Processing

- 16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
- 16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## 17. Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It 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.

- 17.1 The Company processes personal data using automated means. This includes SAGE, 360SiteView, PowerRetrieve, 360Retrieve, OP2 and Withyouin5.
- 17.2 Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the

performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

- 17.3 To facilitate the right of data portability, the Company may make available, as appropriate, all applicable personal data to data subjects or the Data Controller in the following formats:
  - 17.3.1 PDF
  - 17.3.2 JSON
  - 17.3.3 JPEG
  - 17.3.4 MP4

At a minimum we will supply personal data in:

- 17.3.5 A structured, commonly used and machine-readable form. (Machine readable means that the information is structured so that software can extract specific elements of the data.)
- 17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
- 17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

## 18. Objections to Personal Data Processing

- 18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.
- 18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
- 18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.
- 18.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## 19. Automated Decision-Making

- 19.1 The Company does not use personal data in automated decision-making processes.
- 19.2 Where such decisions have a legal (or similarly significant effect) on data subjects,

those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

- 19.3 The right described in Part 19.2 does not apply in the following circumstances:
  - 19.3.1 The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;
  - 19.3.2 The decision is authorised by law; or
  - 19.3.3 The data subject has given their explicit consent.

## 20. Profiling

- 20.1 The Company does not use personal data for profiling purposes.
- 20.2 When personal data is used for profiling purposes, the following shall apply:
  - 20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
  - 20.2.2 Appropriate mathematical or statistical procedures shall be used;
  - 20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
  - 20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

## 21. Personal Data Collected, Held and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy and Addendum):

Data Ref.	Type of Data	Lawful purpose of processing activity and purpose of data processing
Client	Client details (at individual level): a) Identity b) Contact c) Device d) Usage	Performance of a contract, to provide technical support
Customer of Client	Customer details: a) Identity b) Contact c) Device d) Usage	Performance of a contract, to provide technical support
Supplier	Supplier details (at individual level): a) Identity b) Contact c) Device d) Usage	Performance of a contract, to provide technical support
WYi5 Agent	Agent details: a) Identity b) Contact c) Device d) Usage	Performance of a contract, to provide technical support
Employee	Employee details: a) Identity b) Contact c) Financial d) Device e) Usage f) Medical	Performance of a contract Necessary to comply with a legal obligation
Clients and Prospective Clients	Details: a) Identity b) Contact c) Usage	Necessary for the Company's legitimate interests (to study how clients use our products and services, to develop them, to grow our business and to refine our marketing strategy)
All users of our products and services	Details: a) Identity b) Contact c) Usage	Necessary for the Company's legitimate interests (use of data analytics to improve our products and services, marketing, customer and client relationships and experiences)

## 22. Data Security – Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- 22.1 All emails containing personal data must be encrypted. Currently they are encrypted with TLS 1.2 which is a feature of Exchange online
- 22.2 Emails containing personal data and personal data attachments, which are as a direct consequence from a SAR or from Human Resources (HR), must be marked “confidential”;
- 22.3 Personal data may be transmitted over secure networks only;
- 22.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- 22.5 Personal data contained in the body of an email should be stored securely. All files containing personal data and attached to an email should also be deleted from the email, assuming they can be recreated.
- 22.6 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Special Delivery Service; and
- 22.7 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

## 23. Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- 23.1 All electronic copies of personal data must be stored securely either by:
  - 23.1.1 Securing the file using file specific passwords saved on an encrypted drive/folder with appropriate access controls;
  - 23.1.2 Stored within a file management system that uses authenticated login, file level security and encryption in transit and at rest.
  - 23.1.3 Stored within a database with access controls, encryption in transit and at rest and where practicable pseudonymised.
- 23.2 Encryption levels should be appropriate for the technology being utilised (e.g. TLS 1.2 for emails) and the level of sensitivity/ risk of the personal data contained within;
- 23.3 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- 23.4 All personal data stored electronically should be stored within the designated cloud-based file storage for the data type where the back-up of the data is securely managed by the cloud service it is contained within;
- 23.5 Files containing personal data should not be stored on a laptop unless the file location is;

- 23.5.1 Not the system drive;
  - 23.5.2 Not a removable drive;
  - 23.5.3 And is compliant with 23.5.1
- 23.6 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

## 24. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy and addendum.

## 25. Data Security – Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- 25.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested, following the correct procedure, depending on the personal data to be shared.
- 25.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of:
  - As above in 25.1
- 25.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- 25.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- 25.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Marketing to ensure that the appropriate consent is obtained and that no data subjects have opted out.

## 26. Data Security – IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

- 26.1 All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. A password manager is recommended. All software used by the Company is designed to require such passwords.;
- 26.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- 26.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff, or nominated Support IT Centre, shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible unless there are valid technical reasons not to do so; and
- 26.4 No software may be installed on any Company-owned computer or device without the prior approval of 360Globalnet, the individual's immediate manager / supervisor and a member of the board (if the software is to be installed on more than one individual's device(s)). The parties involved must also have taken advice from 360Globalnet's outsourced Support IT Centre who actually enable the software to be installed (if applicable).

## 27. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- 27.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
- 27.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- 27.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- 27.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- 27.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- 27.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- 27.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;



- 27.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- 27.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- 27.10 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and
- 27.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## 28. Transferring Personal Data to a Country Outside the EEA

- 28.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA and outside the protection of the GDPR. This is called a 'restricted transfer'.
- 28.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
  - 28.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
  - 28.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
  - 28.2.3 The transfer is made with the informed consent of the relevant data subject(s);
  - 28.2.4 The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
  - 28.2.5 The transfer is necessary for important public interest reasons;
  - 28.2.6 The transfer is necessary for the conduct of legal claims;
  - 28.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

28.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

28.2.9 The final transfer that may be applied can only apply,

If 360GN:

- are making a one-off restricted transfer in compelling legitimate interests.
- cannot rely on any of the other exceptions  
It
- should not be relied on lightly, never routinely and is
- only for **truly exceptional** circumstances.

For this exception (Exception 8 of Article 49 of the GDPR) to apply to a restricted transfer:

1. there must be no adequacy decision which applies.
2. 360GN are unable to use any of the other appropriate safeguards. Serious consideration must be given to this, even if it would involve significant investment.
3. None of the other exceptions apply. Again, serious consideration must be given to the other exceptions. It may be that explicit consent may be obtained with some effort or investment.
4. The transfer must not be repetitive – that is, it may happen more than once but not regularly.
5. The personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise that must be undertaken.
6. The transfer must be necessary for the compelling legitimate interests. Please see the section in the policy on legitimate interests as a lawful basis for processing but bear in mind that this exception requires a higher standard, as it must be a compelling legitimate interest. The ICO give an example as a transfer of personal data to protect a company's IT systems from serious immediate harm.
7. On balance, 360GN's compelling legitimate interests outweigh the rights and freedoms of the individuals.
8. 360GN has made a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data. Suitable safeguards might be strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes or sending pseudonymised or encrypted data. This must be recorded in full in the documentation of the processing activities.
9. 360GN have informed the ICO of the transfer. They will ask to see full details of all the steps 360GN has taken as set out above.
10. 360GN has informed the individual of the transfer and explained their compelling legitimate interest to them.

## 29. Data Breach Notification

29.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

29.2 If a personal data breach occurs and that breach is likely to result in a risk to the

rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

- 29.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 29.4 Data breach notifications shall include the following information:
- 29.4.1 The categories and approximate number of data subjects concerned;
  - 29.4.2 The categories and approximate number of personal data records concerned;
  - 29.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
  - 29.4.4 The likely consequences of the breach;
  - 29.4.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## 30. Mutual Legal Assistance requests/Judicial Cooperation

Mutual Legal Assistance (MLA) is a method of cooperation between States for obtaining assistance in the investigation or prosecution of criminal offences and does not come under the GDPR. It is mentioned here for completeness of this policy. MLA is generally used for obtaining information that cannot be obtained on a law enforcement (police to police) to basis, particularly enquiries that require coercive means. Requests are made by a formal international Letter of Request (ILOR or LOR). In civil law jurisdictions these are also referred to as Commissions Rogatoires. This assistance is usually requested by courts or prosecutors and is therefore also referred to as 'judicial cooperation'.

MLA can also be used to obtain assistance in the investigation of the proceeds of crime and also in their freezing and confiscation. Proceeds of crime matters can be on a criminal (conviction) basis or a civil (non-conviction) basis.

Due to the increasingly global nature of crime, MLA is critical to criminal investigations and proceedings both in the UK and abroad. The UK is committed to assisting investigative, prosecuting and judicial authorities in combating international crime and is able to provide a wide range of MLA. MLA is also a vital tool in the pursuit of criminal finances including the recovery of the proceeds of crime that may have been moved and hidden assets overseas.

These guidelines are to ensure that requests for MLA received by the UK can be acceded to and executed quickly and efficiently.

### 31. Implementation of Policy

This Policy shall be deemed effective as of 25<sup>th</sup> May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Lorraine Fiander  
Position: Data Protection Officer  
Date: 25<sup>th</sup> February 2020  
Due for Review by: January 2021  
Signature: 