

Data Protection Policy

Version:	1.5
Date:	2022/06/07
Revised by:	L Curry
Approved by:	N Curry

Confidentiality Level:	Public
Date Next Review:	2027/06/06

Contents

1. Introduction 3
2. Obligations 4
3. Data Protection Principles 5
4. Data Subject Rights 6
5. Lawful, Fair and Transparent Data Processing 6
6. Specified, Explicit and Legitimate Purposes 8
7. Adequate, Relevant and Limited Data Processing 9
8. Accuracy of Data and Keeping Data Up to Date 9
9. Data Retention 9
10. Secure Processing 10
11. Accountability and Record Keeping 10
12. Data Protection Impact Assessments 11
13. Keeping Data Subjects Informed 12
14. Data Subject Access 13
15. Rectification of Personal Data 14
16. Erasure of Personal Data 14
17. Restriction of Personal Data Processing 15
18. Data Portability 15
20. Automated Decision Making 16
23. Data Security – Transferring Personal Data and Communications 17
24. Data Security - Storage 18
25. Data Security - Disposal 18
26. Data Security – Use of Personal Data 19
28. Organisational Measures 20
29. Transferring Personal Data to a Country Outside the EEA 21
30. Data Breach Notification 22
31. Implementation of Policy 23
32. Policy Monitoring 23
33. Records and Reports Associated with this Policy 23

1. Introduction

1.1 Scope

The Data Protection Policy applies to all staff, students, partners, subcontractors and visitors to Blue Lights Digital Ltd.[1]

Adherence to this policy forms part of all employment and subcontractor contracts and its contents are not to be regarded by any person as implied.

1.2. Revision History

Ver.	Date	Record of Changes	Created by	Approved By
1.0	2018/06/30	Documentation existing practice	K. Gunther	M Service
1.1	2018/12/30	Reviewed	K. Gunther	M Service
1.2	2019/06/31	Reviewed	K. Gunther	M Service
1.3	2019/12/30	Reviewed	K. Gunther	M Service
1.4	2020/12/31	Reviewed. Minor revisions.	K. Gunther	M Service
1.5	2022/06/07	Reviewed	L Curry	N Curry
1.6	2026/06/07	Reviewed	L Curry	N Curry

1.3. Terms and definitions

- 'we' and 'our' refer to BLD
- 'personal data' is defined by the GDPR 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

[1] Hereafter, referred to as BLD.

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.

- 'records' are those classes of controlled documents that provide evidence of conformity to management system requirements

1.4. Responsibilities

The Data Protection Officer (DPO) is responsible for all aspects of the implementation and management of this procedure, with assistance from the Quality Team unless noted otherwise.

Directors, managers and supervisors are responsible for the implementation of this procedure within the scope of their responsibilities.

All employees, subcontractors and agents of the Company are required to act in a way that does not knowingly breach GDPR and Data Protection Regulations. The co-operation of all employees is essential for the success of this Policy.

The Company takes responsibility for achieving the objectives of this Policy and endeavours to ensure compliance with relevant Legislation and Codes of Practice. The Data Protection Officer owns this document and should review it annually, if not every six months, in conjunction with the ISMS Team. They both have the prime responsibility for sustaining and developing it and for undertaking any day-to-day activities required to sustain it.

24. Obligations

This Policy sets out the obligations of BLUE LIGHTS DIGITAL LTD, a company registered in the United Kingdom under number 09430671, whose registered office is at The Officers' Mess Business Centre, Royston Road, Duxford, Cambridge, CB22 4QH ("the Company") regarding data protection and the rights of our "data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

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 always be followed 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.

25. Data Protection Principles

3.1 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:

25.2. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

25.3. 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 incompatible with the initial purposes.

25.4. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

25.5. 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.

25.6. 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.

25.7. 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.

26. Data Subject Rights

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

26.2. The right to be informed (Part 12).

26.3. The right of access (Part 13).

26.4. The right to rectification (Part 14).

26.5. The right to erasure (also known as the 'right to be forgotten') (Part 15)

26.6. The right to restrict processing (Part 16).

26.7. The right to data portability (Part 17).

26.8. The right to object (Part 18); and

26.9. Rights with respect to automated decision-making and profiling (Parts 19 and 20).

27. Lawful, Fair and Transparent Data Processing

5.1 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:

27.2. The data subject has given consent to the processing of their personal data for one or more specific purposes.

27.3. 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 a contract with them.

27.4. The processing is necessary for compliance with a legal obligation to which the data controller is subject.

27.5. The processing is necessary to protect the vital interests of the data subject or of another natural person.

27.6. 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

27.7. 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, where the data subject is a child.

27.8. 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:

27.9. 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).

27.10. 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).

27.11. 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.

27.12. 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;

27.13. The processing relates to personal data which is clearly made public by the data subject.

27.14. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

27.15. The processing is necessary for substantial public interest reasons, based on 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.

27.16. 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 based on 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.

27.17. 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, based on 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

27.18. 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.

28. Specified, Explicit and Legitimate Purposes

6.1 The Company collects and processes the personal data set out in Part 22 of this Policy. This includes:

28.2. Personal data collected directly from data subjects and

28.3. Personal data obtained from third parties.

28.4. The Company only collects, processes and holds personal data for the specific purposes set out in Part 22 of this Policy (or for other purposes expressly permitted by the GDPR).

28.5. 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 13 for more information on keeping data subjects informed.

29. 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 6, above, and as set out in Part 22, below.

30. Accuracy of Data and Keeping Data Up to Date

30.2. 8.1 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.

30.3. 8.2 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.

31. Data Retention

31.2. 9.1 The Company shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held and processed.

31.3. 9.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

31.4. 9.3 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.***

32. 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 23 to 28 of this Policy.

33. Accountability and Record Keeping

11.1 The Company's Data Protection Officer is Matt Service at:
matt@bluelightsdigital.com

He is supported by the ISMS Team: isms@bluelightsdigital.com

11.2 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.

The Company shall keep written internal records of all personal data collection, holding and processing, which shall incorporate the following information:

11.2.1. The name and details of the Company, its Data Protection Officer and any applicable third-party data processors.

11.2.2. The purposes for which the Company collects, holds and processes personal data.

33.2.3. 11.2.3 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.

33.2.4. 11.2.4.Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.

33.2.5. 11.2.5 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

33.2.6. 11.2.6.Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

34. Data Protection Impact Assessments

34.1. The Company shall carry out Data Protection Impact Assessments for 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.

34.2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

34.2.1. The type(s) of personal data that will be collected, held and processed.

34.2.2. The purpose(s) for which personal data is to be used.

34.2.3. The Company's objectives.

34.2.4. How personal data is to be used.

34.2.5. The parties (internal and/or external) who are to be consulted.

34.2.6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

34.2.7. Risks posed to data subjects.

34.2.8. Risks posed both within and to the Company; and

34.2.9. Proposed measures to minimise and handle identified risks.

35. Keeping Data Subjects Informed

35.1. The Company shall provide the information set out in Part 13.2 to every data subject:

35.2. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

35.3. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

35.3.1. if the personal data is used to communicate with the data subject, when the first communication is made; or

35.3.2. if the personal data is to be transferred to another party, before that transfer is made; or

35.3.3. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

35.4. The following information shall be provided:

35.4.1. Details of the Company including, but not limited to, the identity of its Data Protection Officer.

35.4.2. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 22 of this Policy) and the legal basis justifying that collection and processing.

35.4.3. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data.

35.4.4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.

35.4.5. Where the personal data is to be transferred to one or more third parties, details of those parties.

35.4.6. 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 29 of this Policy for further details).

35.4.7. Details of data retention.

35.4.8. Details of the data subject's rights under the GDPR.

35.4.9. Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time.

35.4.10. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR).

35.4.11. 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

35.4.12. 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.

36. Data Subject Access

36.1. 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.

36.2. Data subjects wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer.

36.3. 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.

36.4. All SARs received shall be handled by the Company's Data Protection Officer with assistance from the ISMS Team.

36.5. 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.

37. Rectification of Personal Data

37.1. Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

37.2. 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.

37.3. If 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.

38. Erasure of Personal Data

38.1. Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

38.1.1. 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.

38.1.2. The data subject wishes to withdraw their consent to the Company holding and processing their personal data.

38.1.3. 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 19 of this Policy for further details concerning the right to object).

38.1.4. The personal data has been processed unlawfully.

38.1.5. The personal data needs to be erased for the Company to comply with a particular legal obligation or

38.1.6. The personal data is being held and processed for the purpose of providing information society services to a child.

38.2. 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.

38.3. If 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).

39. Restriction of Personal Data Processing

39.1. 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.

39.2. If 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).

40. Data Portability

Currently, the Company does not process personal data using automated means but this section has been retained so that it will be re-considered upon each review.

41. Objections to Personal Data Processing

19.1 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.

19.2 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.

19.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately. 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.

42. Automated Decision Making

At this time, the Company does not use personal data in automated decision making but this section has been retained so that it will be re-considered upon each review.

43. Profiling

At this time, the Company does not use personal data in automated decision making but this section has been retained so that it will be re-considered upon each review.

44. Personal Data Collected, Held and Processed (Does this section need each bullet numbering)

We may collect some or all of the following personal data (this may vary according to your relationship with us):

name.

force/agency/business/company name.

rank, title, position.

contact information such as email addresses and telephone numbers.

demographic information such as post code, preferences and interests.

financial information such as credit / debit card numbers.

IP address.

web browser type and version.

operating system.

a list of URLs starting with a referring site, your activity on Our Site and the site you exit to.

Your personal data may be provided to us by your employment organisation or organisation framework provider when applying for training.

45. 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:

23.1. All emails containing personal data must be encrypted.

45.2. All emails containing personal data must be marked "confidential".

23.3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

23.4. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.

23.5. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email it-self should be deleted. All temporary files associated therewith should also be deleted.

23.6. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax ma-chine to receive the data.

23.7. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a signed for service; and

23.8 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".

46. Data Security - Storage

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

24.1. All electronic copies of personal data should be stored securely using passwords and data encryption.

24.2. 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.

24.3. All personal data stored electronically should be backed up regularly with backups stored offsite. All backups should be encrypted.

24.4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the BLD Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given and for no longer than is necessary; and

24.5. 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).

25. 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.

47. 26. Data Security – Use of Personal Data

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

26.1. 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 from the BLD Data Protection Officer.

26.2. 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 from the BLD Data Protection Officer.

26.3. Personal data must be always handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.

26.4. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it; and

26.5. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the BLD Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

27. Data Security - IT Security

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

27.1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise com-

promised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols and should comply to the procedures outlined in the SYSOP Policy.

27.2. 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.

27.3. All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company's IT staff shall be responsible for installing all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

27.4. No software may be installed on any Company-owned computer or device without the prior approval of the Change Control Board, chaired by the SSO.

28. Organisational Measures

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

28.1. 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.

28.2. Only employees, agents, sub-contractors or other parties working on behalf of the Company that needs access to and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by the Company.

28.3 All employees, agents, contractors or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

28.4. All employees, agents, contractors or other parties working on behalf of the Company handling personal data will be appropriately supervised.

28.5. 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.

28.6. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.

28.7 All personal data held by the Company shall be reviewed periodically as set out in the Company's Data Retention Policy.

28.8. 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.

28.9. 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.

28.10. All agents, contractors or other parties working on behalf of the Company handling personal data must ensure that all 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,

28.11. 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.

48. 29 Transferring Personal Data to a Country Outside the EEA

29.1. The Company may from time-to-time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

29.2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

29.3. 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.

29.4. 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;

29.5. The transfer is made with the informed consent of the relevant data subject(s);

29.6. 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).

29.7. The transfer is necessary for important public interest reasons.

29.8. The transfer is necessary for the conduct of legal claims.

29.9. 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

29.10. 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 can show a legitimate interest in accessing the register.

49. 30. Data Breach Notification

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

30.2. 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.

30.3 If a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 30.2) 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.

30.4. Data breach notifications shall include the following information:

30.5. The categories and approximate number of data subjects concerned.

30.6. The categories and approximate number of personal data records concerned.

30.7. The name and contact details of the Company's Data Protection Officer (or other contact point where more information can be obtained); The likely consequences of the breach; 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.

50. 31. Implementation of Policy

This Policy shall be deemed effective as of 24 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

51. 32. Policy Monitoring

The CEO will receive a report on the implementation of this policy as/if incidents arise. The company reserves the right to amend and update this Policy at any time. The Data Protection Officer owns this document and should review it annually, if not every six months, in conjunction with the ISMS Team.

52. 33. Records and Reports Associated with this Policy

Further development of this policy could include a reporting template and an incident log and an annual board report template.