Data Protection Policy

1. Introduction

This Policy sets out the obligations of Pimbrook Software a company registered in Ireland under number 337258, whose registered office is at 13 Seapoint, Riverstown Business Park, Tramore, Co. Waterford ("the Company") regarding data protection and the rights of all our business contacts i.e. customers, suppliers, partners and agents ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("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 10).

3.2 The right of access (Part 11);

3.3 The right to rectification (Part 12);

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 13);

3.5 The right to restrict processing (Part 14);

3.6 The right to data portability (Part 15);

3.7 The right to object (Part 16); and

3.8 Rights with respect to automated decision-making and profiling (the Company does not currently nor intends to engage in these activities).

4. Lawful, Fair, and Transparent Data Processing

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

4.2 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;

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

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

4.5 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

4.6 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.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in Part 17 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.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 17 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 10 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 17, 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 12 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 Details about the retention period for each type of personal data held by the Company are provided in Part 17 of this Policy.

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 18 to 22 of this Policy.

10. Keeping Data Subjects Informed

10.1 The Company shall provide the information set out in Parts 10.2 and 10.3 to every data subject:

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

10.1.2 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.

10.2 The following information is provided in this Policy:

10.2.1 Details of the Company (as outlined in the Introduction);

10.2.2 The purpose(s) for which the personal data is being collected and will be processed, the legitimate interests and legal basis justifying that collection and processing and the length of time the data will be retained (as detailed in Part 17);

10.2.3 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed (as detailed in Part 17);

10.2.4 The data subject's rights under the GDPR (as outlined in Part 3);

10.2.5 The data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

10.2.6 The data subject's right to complain to the Data Protection Commissioner's Office (the "supervisory authority" under the GDPR);

10.3 Extra information may be provided;

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

10.3.2 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);

10.3.3 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

10.3.4 Where any automated decision-making or profiling that will take place using the personal data, details including information on how decisions will be made, the significance of those decisions, and any consequences.

11. Data Subject Access

11.1 Data subjects may make subject access requests ("SARs") in writing 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.

11.2 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.

11.3 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.

12. Rectification of Personal Data

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

12.2 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.

12.3 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.

13. Erasure of Personal Data

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

13.1.1 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;

13.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

13.1.3 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 16 of this Policy for further details concerning the right to object);

13.1.4 The personal data has been processed unlawfully;

13.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

13.2 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.

13.3 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).

14. Restriction of Personal Data Processing

14.1 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.

14.2 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).

15. Data Portability

15.1 The Company processes personal data using automated means (i.e. computer databases and software systems).

15.2 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).

15.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in a common file format which will be readable and suitable for import into computer applications i.e. comma separated values (CSV).

15.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

15.5 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.

16. Objections to Personal Data Processing

16.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling),

16.2 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.

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

17. Personal Data Collected, Held, and Processed

The following personal data maybe collected, held, and processed by the Company.

Type of Data	Purpose of Data	Legal Basis	Retention Period
Business contact information (i.e. name, company, telephone number, email address.)	For communication on business relationship matters (i.e. accounts administration, buying & selling of goods & services, service of contract, marketing).	Service contract or the legitimate interest of maintaining a working business relationship.	While there is an existing business relationship (i.e. contract, on-going trading or working relationship) and up to 6 years after a business relationship ends (to cover legislative reporting if required, e.g. revenue).
Marketing contact information (i.e. name, company, telephone number, email address.)	For business to business sales and marketing activities.	Consent	12 months after last communication.
Data related to software we support (i.e. accounts or payroll data sent to us for investigation or fixing).	To fulfil our customer support service agreements we may need to investigate issues related to this data and/or fix corrupted data.	Service contract	For the length of time required to complete the job related to the specific issue raised by the customer.

18. 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:

18.1 Electronic personal data will be transfer using secure methods (e.g. encryption and/or password protection).

18.2 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" and passed directly to the recipient.

19. Data Security - Storage

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

19.1 All electronic copies of personal data should be stored securely on the Company systems and will be protected by appropriate security measures (i.e. firewall and passwords). Backups will be taken regularly to protect against loss due to system failure and data corruption;

19.2 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;

20. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason it should be securely deleted and disposed of.

21. **Data Security - Use of Personal Data**

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

21.1 All authorised parties of the Company (i.e. employees, contractors, agents) should be instructed on how to handle any personal data with care in accordance of the principles outlined in this policy.

21.2 No personal data should be shared with parties not authorised by the Company;

21.3 No personal data should be left on view or unattended for any period of time.

22. **Organisational Measures**

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

22.1 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;

22.2 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;

22.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be appropriately trained to do so;

22.4 All employees, agents, contractors or other parties working on behalf of the Company is subject to a duty of confidentiality;

22.5 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;

22.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

22.7 All personal data held by the Company shall be reviewed periodically;

23. **Transferring Personal Data to a Country Outside the EEA**

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

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

23.2.1 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;

23.2.2 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;

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

23.2.4 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);

23.2.5 The transfer is necessary for important public interest reasons;

23.2.6 The transfer is necessary for the conduct of legal claims;

23.2.7 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

23.2.8 The transfer is made from a register that, under Irish 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.

24. Data Breach Notification

24.1 All personal data breaches must be reported immediately to the Company's Operations Director or any other director available at the time.

24.2 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 Company's board of directors must inform the Data Protection Commissioners Office in Ireland of the breach within 72 hours after having become aware of it.

24.3 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 24.2) to the rights and freedoms of data subjects, the Company must ensure that all affected data subjects are informed of the breach directly and without undue delay.

24.4 Data breach notifications shall include the following information:

24.4.1 The categories and approximate number of data subjects concerned;

24.4.2 The categories and approximate number of personal data records concerned;

24.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

24.4.4 The likely consequences of the breach;

24.4.5 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.

25. Implementation of Policy

This Policy shall be deemed effective as of 25/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date. This policy may be updated as required over time to keep in line with data protection regulation and Company policy.

26. Contact Details

You can contact us with any queries relating to this policy or to exercise any of your rights using the following contact details:

Online: www.pimbrook.ie/

Email: info@pimbrook.ie

Phone: +353 51 395900

Address: 13 Seapoint, Riverstown Business Park, Tramore, Co. Waterford.

Dated: 19/11/2019