

< D	S A M P L E	> y
--------	----------------------------	--------

1. Introduction

This Policy sets out the Company's approach to the collection, use, storage, and disposal of personal data of individuals (physical or legal persons) registered in <<insert company registration number>>, within the Company's jurisdiction (the "Company") regarding data subjects, e.g. staff, customers, suppliers, etc. This Policy sets out the Company's approach to the collection, use, storage, and disposal of personal data under the applicable data protection legislation and regulations, including the EU General Data Protection Regulation (the "EU GDPR") and the UK General Data Protection Regulation (the "UK GDPR"), as it applies in Northern Ireland by virtue of the Data Protection Act 2018 and the Data Protection Regulations 2018 as amended.

This Policy sets the Company's approach to the collection, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed by the Company, its employees, agents, contractors, or other parties.

<<insert company name>>, a company registered in <<insert company registration number>> under number <<insert company registration number>> is at <<insert address>> ("the Company"). This Policy sets out the Company's approach to the collection, use, storage, and disposal of personal data of individuals (physical or legal persons) registered in <<insert company registration number>>, within the Company's jurisdiction (the "Company") regarding data subjects, e.g. staff, customers, suppliers, etc. This Policy sets out the Company's approach to the collection, use, storage, and disposal of personal data under the applicable data protection legislation and regulations, including the EU General Data Protection Regulation (the "EU GDPR") and the UK General Data Protection Regulation (the "UK GDPR"), as it applies in Northern Ireland by virtue of the Data Protection Act 2018 and the Data Protection Regulations 2018 as amended.

This Policy sets the Company's approach to the collection, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed by the Company, its employees, agents, contractors, or other parties.

2. Definitions

"consent"

consent of the data subject which is freely given, specific, informed, and unambiguous indication of the data subject's agreement which they, by a statement or by a positive action, signify their agreement to the processing of personal data relating to

"data controller"

any natural or legal person or persons, which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to the Company, its employees, agents, business contacts etc.>> used in the Company's business for our commercial purposes;

"data processor"

any natural or legal person or persons, which processes personal data on behalf of the data controller;

"data subject"

any living, identified, or identifiable natural person about whom the Company processes personal data;

“EEA”

“personal data”

“personal data breach”

“processing”

“pseudonymisation”

“special category person

3. Scope

3.1 The Company is committed to the spirit of the law and the fair handling of all personal data of all individuals with whom we do business.

3.2 The Company's Data Protection Officer (<<insert name of data protection officer>>), <<insert name of data protection officer>>, is responsible for administering and ensuring compliance with any applicable relevant data protection laws and/or guidelines.

S

A

M

P

L

E

European Economic Area, and all EU Member States, Iceland, Liechtenstein, and Norway;

information relating to a data subject which can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;

breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed;

any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or otherwise making available, alignment or correction, restriction, erasure or destruction;

processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and access to technical and organisational measures ensure that the personal data is not attributed to an identified or identifiable natural person; and

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, sexual life, sexual orientation, or health data.

the letter of the law, but also to the spirit of the law, and to ensure compliance with the correct, lawful, and fair handling of all personal data, and to protect the legal rights, privacy, and trust of all individuals with whom we do business.

<<insert name of data protection officer>>, <<insert name of data protection officer>>, is responsible for administering and ensuring compliance with any applicable relevant data protection laws and/or guidelines.

E

- | | |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.4 | Any questions relating to the Data Protection Law should be referred to the Data Protection Officer should always be consulted. In particular, the Data Protection Officer should always be consulted in the following cases: |
| a) | if there is an issue as to the lawful basis on which personal data is to be processed; |
| b) | if consent is the lawful basis for the collection, holding, and/or processing of personal data; |
| c) | if there is a question as to the retention period for any particular type of personal data; |
| d) | if any new privacy notices or similar privacy-related documentation is to be developed; |
| e) | if any assistance is sought in dealing with the exercise of a data subject's right of access, or if access requests are received; |
| f) | if a personal data breach (whether or actual) has occurred; |
| g) | if there is a question as to security measures (whether technical or organisational) to protect personal data; |
| h) | if personal data is to be shared with third parties (whether such third parties are data controllers or data processors); |
| i) | if personal data is to be transferred outside of the UK and there are questions relating to how to do so; |
| j) | when any significant new processing activity is to be carried out, or when there is a change to existing processing activities, which will require a Data Protection Impact Assessment; |
| k) | when personal data is to be used for purposes different to those for which it was originally collected; |
| l) | if any automated processing, including profiling or automated decision-making, is to be implemented; |
| m) | if any assistance is sought in complying with the law applicable to direct marketing. |

4. The Data Protection Principles

This Policy aims to ensure out the following principles Data controllers are responsible for compliance. All personal data

- 4.1 processed lawfully, in a transparent manner in relation to the data subject;
- 4.2 collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further

S

processing for archiving in the public interest, scientific or historical research purposes shall not be considered to be incompatible with the rights of the data subject.

4.3 adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed;

4.4 accurate and, where necessary, up to date. Every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which the data are processed, or rectified without delay;

4.5 kept in a form which allows 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 in a form which permits processing solely for the purposes of the public interest, scientific or historical research purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject;

4.6 processed in a manner which 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.

5. The Rights of Data Subjects

The UK GDPR sets out the rights applicable to data subjects:

5.1 The right to be informed;

5.2 the right of access;

5.3 the right to rectification;

5.4 the right to erasure ('the right to be forgotten');

5.5 the right to restrict processing;

5.6 the right to data portability;

5.7 the right to object; and

5.8 rights with respect to automated decision making and profiling.

6. Lawful, Fair, and Transparent Processing

6.1 Data Protection Law requires that personal data is processed lawfully, fairly, and transparently in relation to the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following conditions is met:

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

b) the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;

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

A

M

P

L

S

- d) the processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) 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 controller;
- f) the processing is necessary for purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject, in particular where the data subject is a child;

6.2 [If the personal data are of a special category (also known as "sensitive personal data"), the following conditions must be met:

- a) the data subject has given explicit consent to the processing of such data for one or more specific purposes (unless the law prohibits the controller from obtaining the consent of the data subject);
- b) the processing is necessary for the purpose of carrying out the obligations and responsibilities of the controller in the field of employment, social security, and social protection law, where the controller is authorised by law or a collective agreement to process the data and provides for appropriate safeguards for the fundamental rights of the data subject;
- c) 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;
- d) the data controller is a non-profit association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is necessary for the purposes of its legitimate activities, provided that the data are processed solely to the members or former members of the association or body who have regular contact with it in connection with those activities and that the personal data is not made available to a third party without the consent of the data subjects;
- e) the processing is necessary for data which is manifestly made public by the data subject;
- f) the processing is necessary for the conduct of legal claims or for the exercise or defence of legal capacity;
- g) the processing is necessary on substantial public interest reasons, on the basis of which the controller, proportionate to the aim pursued, shall implement appropriate and effective data protection measures, and shall provide for appropriate safeguards the fundamental rights and freedoms of the data subject;
- h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for the provision of health or social care or treatment, or for the management of health or social care systems or services, pursuant to a contract with a health professional, where the processing is subject to specific conditions and safeguards referred to in Article 9(3) of the GDPR.

A

M

P

L

E

- i) the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, including serious cross-border threats to health care, on the basis of law which provides specific measures to safeguard the rights and interests of the subject (in particular, professional secrecy); or
- j) the processing is necessary for reasons of public interest, such as archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with article 89(1) of the UK GDPR (as implemented by the Data Protection Act 2018) based on the aim pursued, respect the essence of the rights and freedoms, and provide for suitable and effective safeguards to protect the fundamental rights and the interests of the data subject.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following conditions must be met:

- 7.1 Consent is a clear affirmative action indicating the data subject that they agree to the processing of their personal data. Consent may take the form of a statement or a pre-ticked box, but pre-ticked boxes, or inactivity are unlikely to amount to consent.
- 7.2 Where consent is one of the lawful bases, it must be clearly separate from such other matters, which includes other matters, the consent must be clearly separate from such other matters.
- 7.3 Data subjects are free to withdraw their consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- 7.4 If personal data is transferred to a third party for a purpose that is incompatible with the purpose for which the data was originally collected that was not within the scope of their consent, consent must be obtained from the data subject.
- 7.5 [If special category data is processed, the Company shall normally rely on a lawful basis other than consent. If explicit consent is relied upon, the data subject must be issued with a suitable privacy notice in order to ensure that they are aware of the nature of the processing.]
- 7.6 In all cases where consent is the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to demonstrate compliance with consent requirements.

8. Specified, Explicit, and Legitimate Interests

- 8.1 The Company collects and processes personal data set out in Part 24 of this Policy. This includes:
 - a) personal data of data subjects[.] OR [; and]
 - b) [personal data of data subjects.]

S

8.2 The Company only holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by law).

8.3 Data subjects must be informed of the purposes of the purpose or purposes for which the Company holds their personal data. Please refer to Part 15 for more information on how this will be done.

9. Adequate, Relevant, and Necessary

9.1 The Company will only hold personal data for and to the extent necessary for the specific purposes of which data subjects have been informed (or which have been set out in Part 8, above, and as set out in Part 24, below).

9.2 Employees, agents, and other parties working on behalf of the Company may collect, process, and hold personal data to the extent required for the performance of their duties in accordance with this Policy. Excessive personal data will not be collected.

9.3 Employees, agents, and other parties working on behalf of the Company may process personal data when the performance of their job duties requires it. Personal data that the Company cannot be processed for any unrelated reason will not be collected.

10. Accuracy of Data and Keeping it up to Date

10.1 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. Please refer to Part 17, below.

10.2 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, the Company shall take reasonable steps to be taken to correct it as appropriate.

11. Data Retention

11.1 The Company shall not retain personal data for any longer than is necessary in light of the purpose for which that personal data was originally collected, held, and processed.

11.2 When personal data is no longer necessary, all reasonable steps will be taken to delete or otherwise destroy the data.

11.3 For full details of the Company's data retention periods for different types of personal data, please refer to our Data Retention Policy.

12. Secure Processing

12.1 The Company shall ensure that all personal data collected, held, and processed is kept secure against unauthorised or unlawful access, use, disclosure, destruction, or damage. Further details of the technical and organisational measures which shall be taken are set out in Part 18, below.

A

M

P

L

E

S

A

M

P

L

E

provided in Parts 25

12.2 All technical and or be regularly reviewed the continued secur

12.3 Data security must integrity, and availa

a) only those v who are auth

b) personal da purposes for

c) authorised u required for

ken to protect personal data shall re their ongoing effectiveness and

es by protecting the confidentiality, as follows:

ccess and use personal data and ess and use it;

and suitable for the purpose or d, and processed; and

le to access the personal data as r purposes.

13. Accountability and Reco

13.1 The Data Protection developing and im and/or guidelines.

13.2 The Company sha collecting, holding, Assessments shall to the rights and fre information).

13.3 All employees, age Company shall be addressing the rele other applicable Co

13.4 The Company's da evaluated by means

13.5 The Company sha collection, holding, information:

a) the name an any applicab other data co

b) the purpose personal da

c) the Compar consent, the such consen

d) details of t processed b which that p

e) details of an all mechanis

f) details of ho (please refe

or administering this Policy and for ble related policies, procedures,

esign approach at all times when al data. Data Protection Impact ccessing presents a significant risk (please refer to Part 14 for further

r parties working on behalf of the g in data protection and privacy, Protection Law, this Policy, and all

e shall be regularly reviewed and ts.

al records of all personal data n shall incorporate the following

y, its Data Protection Officer, and ers (including data processors and onal data is shared);

ny collects, holds, and processes

es (including, but not limited to, hning such consent, and records of and processing personal data;

onal data collected, held, and he categories of data subject to

data to non-UK countries including rds;

will be retained by the Company Retention Policy);

- g) details of personnel involved in processing and holding location(s);
- h) detailed description of technical and organisational measures taken by the Company to ensure the security of personal data.

14. **Data Protection Impact Assessment and Privacy by Design**

14.1 In accordance with the principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data, including the use of new technologies and where the processing is likely to result in a high risk to the rights and freedoms of data subjects.

14.2 The principles of privacy shall be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

- a) the nature, scope, and purpose or purposes of the collection, holding, and processing;
- b) the state of the art of data protection technical and organisational measures to protect personal data;
- c) the cost of implementing measures; and
- d) the risks posed to the rights and freedoms of data subjects, including their likelihood and severity.

14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address:

- a) the type(s) of personal data to be collected, held, and processed;
- b) the purpose(s) for which the data is to be used;
- c) the Company's legal basis for processing;
- d) how personal data will be stored;
- e) the parties (internal and external) who are to be consulted;
- f) the necessity and proportionality of the data processing with respect to the purpose(s);
- g) risks posed to the rights and freedoms of data subjects;
- h) risks posed to the Company; and
- i) proposed measures to mitigate or handle identified risks.

15. **Keeping Data Subjects Informed**

15.1 The Company shall ensure that the information set out in Part 15.2 to every data subject:

- a) where personal data is collected directly from data subjects, those data subjects will be informed at the time of collection; and
- b) where personal data is collected from a third party, the relevant data subjects will be informed before the data is used:
 - i) if the data subject is to be contacted to communicate with the data subject; or

S

- ii) if the data is transferred to another party, before that transfer;
- iii) as soon as the data is obtained.

15.2 The following information must be provided to data subjects in the form of a privacy notice:

- a) details of the Company, not limited to, contact details, and the names and titles of applicable representatives and its Data Protection Officer;
- b) the purpose(s) for which the personal data is being collected and will be processed (including the purposes of this Policy) and the lawful basis justifying that processing;
- c) where applicable, the legal basis upon which the Company is processing the personal data;
- d) where the personal data is obtained directly from the data subject, the categories of personal data collected and processed;
- e) where the personal data is transferred to one or more third parties, details of those parties;
- f) where the personal data is transferred to a third party that is located outside the UK, details of that transfer, including but not limited to the identity of the third party (see Part 31 of this Policy for further details);
- g) details of any retention periods;
- h) details of the Company's compliance with the UK GDPR;
- i) details of the data subject's right to withdraw their consent to the processing of their personal data at any time;
- j) details of the data subject's right to complain to the Information Commissioner;
- k) where the personal data is obtained directly from the data subject, details about the source of that data;
- l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of the consequences of failing to provide it; and
- m) 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.

A

M

P

L

E

16. Data Subject Access

- 16.1 Data subjects may request more information about the Company's processing of their personal data and it is doing with that information.
- 16.2 Employees wishing to access their personal data should do so using a Subject Access Request Form, sent to the Company's Data Protection Officer at <<insert contact details>>.
- 16.3 Responses to SARs must be made within one month of receipt,

S

A

M

P

L

E

however, this may be extended to two months if the SAR is complex and/or numerous requests are received from the data subject shall be

two months if the SAR is complex and/or numerous requests are received from the data subject shall be

16.4 All SARs received shall be handled in accordance with the Company's Data Protection Officer [and in accordance with the Data Subject Access Request Policy & Procedure].

Company's Data Protection Officer Data Subject Access Request Policy

16.5 The Company does not charge any fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has been provided to a data subject, and for requests that are manifestly unfounded, particularly where such requests are repetitive.

the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has been provided to a data subject, and for requests that are manifestly unfounded, particularly where such requests are repetitive.

17. Rectification of Personal Data

17.1 Data subjects have the right to request the Company to rectify any of their personal data that is inaccurate.

the Company to rectify any of their personal data that is inaccurate.

17.2 The Company shall inform the data subject of that rectification. The Company of the issue shall be informed. In the case of complex requests, the data subject shall be informed.

data in question, and inform the data subject of that rectification. The Company of the issue shall be informed. In the case of complex requests, the data subject shall be informed.

17.3 In the event that personal data has been disclosed to third parties, those parties shall be informed of the rectification to that personal data.

data has been disclosed to third parties, those parties shall be informed of the rectification to that personal data.

18. Erasure of Personal Data

18.1 Data subjects have the right to request the Company to erase the personal data it holds about them in the following circumstances:

the Company erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for the Company to hold that personal data with respect to the purposes for which it was originally collected or processed;
- the data subject has withdrawn their consent to the Company holding and processing that personal data;
- the data subject has objected to the Company holding and processing their personal data and the Company has no overriding legitimate interest to allow the holding and processing of that personal data; Part 21 of this Policy for further details concerning the Company's assessment;
- the personal data has been processed unlawfully;
- the personal data has been processed in order for the Company to comply with a legal obligation;
- [the personal data has been processed for the purpose of marketing to a child.]

Company to hold that personal data in the following circumstances: it was originally collected or processed;

their consent to the Company holding and processing their personal data;

Company holding and processing their personal data in the following circumstances: it was originally collected or processed;

unlawfully;

in order for the Company to comply with a legal obligation; OR [.]

and processed for the purpose of marketing to a child.]

18.2 Unless the Company is legally obliged to do so, it reserves the right to refuse to erase personal data, all requests for erasure shall be handled in accordance with the Company's Data Protection Policy. The data subject shall be informed of the erasure of the data subject's personal data. The period for the Company to respond to the request shall be up to two months in the case of complex requests. The data subject shall be informed.

to refuse to erase personal data, all requests for erasure shall be handled in accordance with the Company's Data Protection Policy. The data subject shall be informed of the erasure of the data subject's personal data. The period for the Company to respond to the request shall be up to two months in the case of complex requests. The data subject shall be informed.

- 18.3 In the event that an individual requests that their personal data be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the request and, if it is not possible or would require disproportionate effort, shall be required to delete the data from their records.
19. **Restriction of Personal Data Processing**
- 19.1 Data subjects may request the restriction of the processing of their personal data it holds about them. Where a data subject makes such a request, the Company shall retain the personal data concerning that data subject (if any) that the data subject has consented to that the personal data in question is not processed further for the purposes for which it was collected.
- 19.2 In the event that personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless this would require disproportionate effort to do so).
20. **[Data Portability]**
- 20.1 The Company provides details of automated processing using automated means. <<Insert details of automated processing>>
- 20.2 Where data subjects request that the Company process their personal data in support of the performance of a contract with the data subject, the Company and the data subject, in accordance with Article 17 of the GDPR, to receive a copy of their personal data and to transmit it to other data controllers).
- 20.3 To facilitate the right to data portability, the Company shall make available all applicable personal data in the following format[s]:
- a) <<list format[s]>>
 - b) <<add further details of format[s]>>
- 20.4 Where technically feasible, personal data shall be sent directly to the data subject, personal data shall be sent to the data subject.
- 20.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. This 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.
21. **Objections to Personal Data Processing**
- 21.1 Data subjects have the right to object to the Company processing their personal data based on its legitimate interests, for direct marketing (including profiling), [and processing for purposes of historical research and statistics purposes].
- 21.2 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 the Company can demonstrate that the Company's legitimate interests override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

- 21.3 Where a data subject has objected to the Company's processing of their personal data for direct marketing purposes, the Company shall cease such processing promptly.
- 21.4 [Where a data subject has objected to the Company's processing of their personal data for scientific and/or statistical purposes, the data subject must, under the particular circumstances, demonstrate grounds relating to his or her objection which are not overridden by the requirements required to comply if the research is carried out for reasons of public interest.]
22. **[Automated Processing, Decision-Making, and Profiling]**
- 22.1 [The Company uses automated decision-making processes as follows:
- a) <<Insert details of automated decision-making>>.]
- 22.2 [The Company uses automated decision-making processes for the following purposes as follows:
- a) <<Insert details of automated decision-making>>.]
- 22.3 The activities described in 22.1 and 22.2 are generally prohibited under Data Protection Law where the processing has a legal or similarly significant effect on the data subject, unless one of the following applies:
- a) the data subject has given explicit consent;
 - b) the processing is necessary for the performance of a contract between the Company and the data subject;
 - c) the processing is necessary for the entry into, or performance of, a contract between the Company and the data subject.
- 22.4 If special category data is processed in this manner, such processing can only be lawful if one of the following applies:
- a) the data subject has given explicit consent;
 - b) the processing is necessary for reasons of substantial public interest.
- 22.5 Where decisions are made using automated processing (including profiling), data subjects must be provided the right to object, to challenge such decisions, to request human intervention, to state their own point of view, and to obtain an explanation of the logic involved. The Company. Data subjects must be explicitly informed of this right at the point of contact.
- 22.6 In addition to the above, the Company must be provided to data subjects an explanation of the logic involved in the decision-making or profiling, and the significance and consequences of the decision or decisions.
- 22.7 When personal data is processed using automated processing, automated decision-making, or profiling, the following measures shall apply:
- a) appropriate technical and organisational measures shall be used;
 - b) technical and organisational measures shall be implemented to minimise the risk of a data breach occurring, such measures must enable the Company to respond to a data breach in this manner shall be secured in order to protect the data subjects arising (see Parts 25 to 30 of this Policy for details of the data security and organisational measures).]

23. **[Direct Marketing**

- 23.1 The Company is subject to applicable laws and regulations when marketing its [products] **AND/OR** services.
- 23.2 The prior consent of the data subject is required for electronic direct marketing including email, text messages and automated telephone calls subject to the following limited exceptions:
- a) The Company may send text messages or emails to a customer if their contact details have been obtained in the context of the marketing relates to similar products or services and the data subject in question has been given the opportunity to opt out when their details were first collected and used for communication from the Company.
- 23.3 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and accessible form and must be kept separate from other information in the marketing communication.
- 23.4 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of data may be retained in such circumstances to ensure that the data subject's marketing preferences are correctly recorded with.]

24. **Personal Data Collected, Stored and Processed**

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

Data Ref.	Type of Data	Details of Data
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>
<<insert ref>>	<<insert data type>>	<<insert details of data>>

25. **Data Security - Transfer of Data to Third Parties and Communications**

The Company shall ensure appropriate security measures are taken with respect to all personal data:

- 25.1 All emails containing personal data shall be encrypted [using <<insert type(s) of encryption>>];

- 25.2 All emails containing personal data shall be marked “confidential”;
- 25.3 Personal data may only be transmitted over secure networks only; transmission over unsecured networks shall be avoided in any circumstances;
- 25.4 Personal data may only be transmitted over a wireless network if there is a wired alternative that is available;
- 25.5 Personal data contained in email shall be copied from email, whether sent or received, to a secure network and stored securely. The email and any data associated therewith should also be deleted [using <<insert name(s)>>];
- 25.6 Where personal data is transmitted via facsimile transmission the recipient shall be informed of the transmission and should be waiting by the fax machine to receive the data;
- 25.7 Where personal data is transmitted in hardcopy form it should be passed directly to the recipient or to a secure delivery service>>];
- 25.8 All personal data transmitted in removable electronic form shall be stored in a suitable container marked “confidential”;
- 25.9 [<<Add further security measures>>].

26. Data Security - Storage

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

- 26.1 All electronic copies of personal data shall be stored securely using <<insert name(s)>> data encryption;
- 26.2 All hardcopies of personal data shall be stored securely in a locked box, drawer, cabinet, or similar;
- 26.3 All personal data shall be backed up <<insert interval>> [using <<insert name(s)>>] offsite]. All backups should be stored securely in a locked box, drawer, cabinet, or similar;
- 26.4 No personal data shall be stored on a mobile device (including, but not limited to, laptops, tablets, or smartphones), whether such device belongs to the Company or on behalf of the Company without the formal written approval of <<insert name(s)>> and, in the event of such approval, strictly in accordance with the instructions and limitations described in the policy or no longer than is absolutely necessary];
- 26.5 No personal data shall be stored on any device personally belonging to an employee, agent, contractor, or third party working on behalf of the Company and transferred to devices belonging to the Company on behalf of the Company where the transfer is not in full compliance with the letter and spirit of this Policy and of the Data Protection Act 1998 (which may include demonstrating to the recipient that appropriate technical and organisational measures have been taken to protect the data);
- 26.6 [<<Add further security measures>>].

S

27. **Data Security - Disposal**

When any personal data (including where copies have been made) is no longer needed, it should be securely deleted and disposed of. For more information on the deletion and disposal of personal data, please refer to the Data Retention Policy.

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

A

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

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

appropriate measures are taken with respect to the use of personal data:

28.1 No personal data should be formally accessed by any employee, agent, contractor, or other party, whether or not, without the appropriate name(s) and/or position(s) and contact details>>;

formally accessed by any employee, agent, contractor, or other party, whether or not, without the appropriate name(s) and/or position(s) and contact details>>;

28.2 No personal data should be formally accessed by any employee, agent, contractor, or other party, whether or not, without the appropriate name(s) and/or position(s) and contact details>>;

formally accessed by any employee, agent, contractor, or other party, whether or not, without the appropriate name(s) and/or position(s) and contact details>>;

28.3 Personal data must not be left unattended or on the desk of any employee, agent, contractor, or other parties at any time.

Personal data must not be left unattended or on the desk of any employee, agent, contractor, or other parties at any time.

28.4 If personal data is left on a computer screen and the computer is left unattended for a period of time, the user must lock the computer and screen.

If personal data is left on a computer screen and the computer is left unattended for a period of time, the user must lock the computer and screen.

28.5 Where personal data is used for marketing purposes, it shall be the responsibility of the Company to ensure that the appropriate consent is obtained from the individual or via a third-party service provider.

Where personal data is used for marketing purposes, it shall be the responsibility of the Company to ensure that the appropriate consent is obtained from the individual or via a third-party service provider.

28.6 [<<Add further security measures>>.]

>>.]

M

P

29. **Data Security - IT Security**

The Company shall ensure appropriate measures are taken with respect to IT and information security:

appropriate measures are taken with respect to IT and information security:

29.1 All passwords used should not be easily guessed or otherwise compromised. All passwords should be a combination of uppercase and lowercase letters, numbers, and special characters. All software used by the Company should be kept up-to-date and secure.

All passwords used should not be easily guessed or otherwise compromised. All passwords should be a combination of uppercase and lowercase letters, numbers, and special characters. All software used by the Company should be kept up-to-date and secure.

29.2 Under no circumstances should passwords be written down or shared between any employee, agent, contractor, or other parties working on behalf of the Company. If a password is forgotten, it must be reset using a secure method. IT staff do not have access to passwords.

Under no circumstances should passwords be written down or shared between any employee, agent, contractor, or other parties working on behalf of the Company. If a password is forgotten, it must be reset using a secure method. IT staff do not have access to passwords.

29.3 All software (including applications and operating systems) should be kept up-to-date and secure. IT staff shall be responsible for installing any and all updates [not more than <<insert

applications and operating systems) should be kept up-to-date and secure. IT staff shall be responsible for installing any and all updates [not more than <<insert

E

30. Organisational Measures

The Company shall ensure the security of personal data collection, holding, and processing.

30.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be notified of their individual responsibilities and the Company's responsibilities under the Data Protection Law and under this Policy, and shall be required to comply with this Policy;

30.2 Only employees, agents, contractors, or other parties working on behalf of the Company that need to process personal data in order to carry out their assigned duties shall be granted access to personal data held by the Company;

30.3 All sharing of personal data with third parties shall be subject to the consent of such data subjects shall be obtained prior to the sharing of personal data;

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

30.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be appropriately supervised;

30.6 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 in the workplace or otherwise;

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

30.8 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Policy;

30.9 The performance of employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

30.10 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be bound to do so in accordance with the principles of Data Protection Policy by contract;

30.11 All agents, contractors, or other parties working on behalf of the Company handling personal data and all of their employees who are involved in the processing of personal data are held to the same conditions as those set out in the Company's Policy and Data Protection Policy;

30.12 Where any agent, contractor, or other party working on behalf of the Company handling personal data breaches the conditions under this Policy that party shall indemnify and hold the Company against any costs, liability,

available by the publisher or manufacturer] OR [if not available, and practically possible] [, unless there are valid technical reasons];

company-owned computer or device or mobile telephone number, department or position>>;

[<<Add further security measures>>].]

measures are taken with respect to the security of personal data.

for parties working on behalf of the Company shall be notified of their individual responsibilities and the Company's responsibilities under the Data Protection Law and under this Policy;

for parties working on behalf of the Company that need to process personal data in order to carry out their assigned duties shall be granted access to personal data held by the Company;

with the information provided to the data subjects. The consent of such data subjects shall be obtained prior to the sharing of personal data;

for parties working on behalf of the Company shall be appropriately trained to do so;

for parties working on behalf of the Company shall be appropriately supervised;

for parties working on behalf of the Company shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters in the workplace or otherwise;

processing personal data shall be regularly evaluated and reviewed;

shall be reviewed periodically, as set out in the Company's Policy;

agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

for parties working on behalf of the Company shall be bound to do so in accordance with the principles of Data Protection Policy by contract;

working on behalf of the Company and all of their employees who are involved in the processing of personal data are held to the same conditions as those set out in the Company's Policy arising out of this Policy;

working on behalf of the Company shall be bound to do so in accordance with the conditions under this Policy that party shall indemnify and hold the Company against any costs, liability,

damages, loss, claim

30.13 [

31. Transferring Personal Data from the UK

31.1 The Company may transfer personal data to a third party (a 'transfer' includes making available remotely) in countries outside of the UK. The UK GDPR restricts such transfers to ensure that the level of protection given to data subjects is not lower than that provided in the UK.

31.2 Personal data may be transferred to a country outside the UK if one of the following applies:

- a) The UK has ensured an adequate level of protection of personal data in its laws, regulations, decisions or administrative arrangements. From 1 January 2021, transfers of personal data to the UK from EEA countries will continue to be permitted. The UK will also be in place to recognise pre-existing EU data protection law in the UK.
 - b) Appropriate safeguards, including binding corporate rules, standard contractual clauses, or approved certification mechanisms, are in place for use in the UK (this includes those adopted prior to 1 January 2021), and an approved certification mechanism.
 - c) The transfer is based on the informed and explicit consent of the data subject.
 - d) The transfer is necessary for one or more of the other reasons set out in the UK GDPR including: for the performance of a contract between the data subject and the controller; for the protection of public interest reasons; for the establishment, exercise or defence of legal claims; to protect the vital interests of the data subject or another person; or, in limited circumstances, for the performance of a task in the public interest.

32. Data Breach Notification

32.1 All personal data b [REDACTED] ed immediately to the Company's Data Protection Offi [REDACTED]

32.2 If an employee, agent or third party working on behalf of the Company becomes aware of a personal data breach, they must report it to the Company immediately. The Company will investigate it themselves. Any and all evidence relating to the breach in question should be carefully retained.

32.3 If a personal data breach is likely to result in a risk to the rights and freedoms of individuals (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Information Commissioner must ensure that the Information Commissioner is notified of the breach without delay, and in any event, within 72 hours of becoming aware of it.

32.4 In the event that a person is likely to result in a high risk (that is, a higher risk than the person referred to in 32.3) to the rights and freedoms of data subjects, the controller must ensure that all affected data subjects are informed of the high risk and without undue delay.

32.5 Data breach notification

- a) The category of data breach;
- b) The category of data subjects concerned;
- c) The name and position of the Company's data protection officer (or other contact person);
- d) The likely consequences of the breach;
- e) Details of the measures proposed to be taken, by the Company to contain or erase the breach, including, where appropriate, measures to compensate or provide redress to affected data subjects.

Following information:

Number of data subjects concerned;
Number of personal data records concerned;
Company's data protection officer (or other contact person) information can be obtained);
The likely consequences of the breach;
Details of the measures proposed to be taken, by the Company to contain or erase the breach, including, where appropriate, measures to compensate or provide redress to affected data subjects.

33. **Implementation of Policy**

This Policy shall be deemed to have been approved on the date of its adoption and shall have retroactive effect from the date of its adoption.

ert date>>. No part of this Policy shall apply to matters occurring on or after the date of its adoption.

This Policy has been approved and signed by the following person:

Name: <<insert name>>

Position: <<insert position>>

Date: <<insert date>>

Due for Review by: <<insert date>>

Signature: