

S

A

M

P

L

E

1. Introduction

This Policy sets out the registered in <<insert company registration number>>, w Company”) regarding refer Company in accordance Legislation” means all legis the use of personal data a not limited to, the retained ((EU) 2016/679) (the “UK Scotland, and Northern (Withdrawal) Act 2018, th Communications Regulation

The Data Protection Legisl an identified or identifiable person is one who can be an identifier such as a n identifier, or to one or mo mental, economic, cultural,

The Data Protection Legisl known as “sensitive” perso to, data concerning the da membership, genetics, bio orientation.

Under the Data Protection permits the identification o purposes for which the pe may be stored for longer purposes that are in the statistical purposes (subje organisational measures r data).

In addition, the Data Protec be forgotten”. Data subj prevent the processing of t

- a) Where the personal originally collected o
- b) When the data subj
- c) When the data subj Company has no ov
- d) When the personal Protection Legislatio
- e) When the personal

Company name>>, a company under number <<insert company is at <<insert address>> (“the ected, held, and processed by the on Legislation. “Data Protection force from time to time regulatg nic communications including, but general Data Protection Regulation of the law of England and Wales, ction 3 of the European Union 2018, the Privacy and Electronic d any successor legislation.

ata” as any information relating to a subject”). An identifiable natural rectly, in particular by reference to number, location data, an online e physical, physiological, genetic, natural person.

pecial category” personal data (also udes, but is not necessarily limited city, politics, religion, trade union rposes), health, sex life, or sexual

ata shall be kept in a form which longer than is necessary for the d. In certain cases, personal data is to be processed for archiving tific or historical research, or for of the appropriate technical and ction Legislation to protect that

the right to erasure or “the right to their personal data erased (and to following circumstances:

- ed for the purpose for which it was ;
- ent;
- sing of their personal data and the st;
- wfully (i.e. in breach of the Data
- comply with a legal obligation; or

S

- f) Where the personal data is used for services to a child.

the provision of information society

This Policy sets out the type of personal data held by the Company [for <<insert specific purpose(s)>> purposes] and the period(s) for which that personal data is retained, the criteria for establishing when it is to be deleted or otherwise disposed of.

held by the Company [for <<insert specific purpose(s)>>], the criteria for establishing when it is to be deleted or otherwise disposed of.

For further information on the Company's Data Protection Legislation, please refer to the Company's Data Protection Policy.

protection and compliance with the Company's Data Protection Policy.

## 2. Aims and Objectives

2.1 The primary aim of this Policy is to ensure that all personal data held by the Company complies with the requirements of the Data Protection Legislation and to ensure that the rights of data subjects are protected.

limits for the retention of personal data and to ensure that the rights of data subjects are protected. This Policy aims to ensure that the Company complies with the requirements of the Data Protection Legislation and the rights of data subjects.

2.2 In addition to safeguarding personal data under the Data Protection Legislation, this Policy aims to ensure that the Company retains only the minimum amount of personal data necessary for the efficient operation of the Company and the efficiency of management.

of data subjects under the Data Protection Legislation. This Policy aims to ensure that excessive amounts of data are not retained by the Company and that the Company aims to improve the speed and efficiency of management.

## 3. Scope

3.1 This Policy applies to all personal data held [by the Company] <<insert department(s)>> [and by third-party service provider(s)] on the Company's behalf.

held [by the Company] OR [by the Company] AND/OR [for <<insert purpose(s)>>] purposes on the Company's behalf.

3.2 Personal data, as defined in the Data Protection Legislation, is held in the following ways and locations:

OR [the above] is stored in the following ways and locations:

- a) [The Company's servers;]
- b) [Third-party servers <<insert location(s)>>];
- c) [Computers permanently stored at <<insert location(s)>>];]
- d) [Laptop computers used by employees;]
- e) [Computers and mobile devices used by employees, agents, and subcontractors [used in accordance with the Company's Bring Your Own Device ("BYOD") Policy];]
- f) [Physical records stored at <<insert location(s)>>];]
- g) [<<add further storage locations as required>>.]

location(s)>>];

service provider(s)>> and located in <<insert location(s)>>];

Company's premises at <<insert location(s)>>];

s] provided by the Company to its employees, agents, and subcontractors in accordance with the Company's Bring Your Own Device ("BYOD") Policy];]

s)>>];]

s required>>.]

## 4. Data Subject Rights and Data Retention

All personal data held by the Company in accordance with the requirements of the Data Protection Legislation shall be retained for the period set out in the Company's Data Protection Policy.

accordance with the requirements of the Data Protection Legislation, the rights thereunder, as set out in the Company's Data Protection Policy.

A

M

P

L

E

S

4.1 Data subjects are kept informed of their rights, of what personal data the Company holds about them, how that personal data is used [as set out in Parts 12 and 13 of the Company's Data Protection Policy], and how long the Company will hold that data. If no fixed retention period can be determined, the criteria for the retention of the data will be determined).

4.2 Data subjects are given access to their personal data held by the Company including the right to request that their personal data be corrected, updated or disposed of (notwithstanding the retention periods of the Company's Data Retention Policy), the right to restrict the Company's use of their data, [the right to data portability,] and further rights relating to automated decision-making and profiling [, as set out in Parts 14 to 20 of the Company's Data Protection Policy].

5. Technical and Organisational Measures

5.1 The following technical and organisational measures are in place within the Company to protect the security of personal data in accordance with Parts 22 to 26 of the Company's Data Protection Policy:

- a) All emails containing personal data are encrypted;
- b) All emails containing personal data are marked "confidential";
- c) Personal data may be stored on secure networks;
- d) Personal data may be transmitted over a wireless network if there is a reasonable wired alternative.

e) Personal data contained in email, whether sent or received, should be copied from the email and stored securely. The email should be deleted;

f) Where personal data is transmitted via facsimile transmission the recipient should be informed that the data is being transmitted and is waiting to receive it;

g) Where personal data is transmitted in hardcopy form, it should be passed directly to the recipient via a secure delivery service <<insert name(s) and/or type(s)>>.

h) All personal data transmitted in a container marked "confidential" should be transferred in a suitable secure container.

i) No personal data may be accessed or processed unless formally requested from <<insert name(s) and/or type(s)>>.

j) All hardcopies of personal data and any electronic copies stored on physical media should be stored in a secure container.

k) No personal data may be accessed or processed by employees, agents, contractors, or other parties, whether or not working on behalf of the Company, without the prior written approval of the Company.

l) Personal data must be protected at all times and should not be left unattended or on view.

m) Computers used to process personal data must always be locked before being left unattended;

n) No personal data should be stored on a mobile device, whether such device belongs to the Company or not, without the formal written approval of the Company.

A

M

P

L

E

S

<<insert position>>  
limitations described  
is absolutely necessary

accordance with all instructions and  
information given, and for no longer than

- o) [No personal data shall be stored on any device personally belonging to an employee and personal data shall not be transferred to devices belonging to agents, contractors or other third parties working on behalf of the Company where the party in question does not comply fully with the Company's Data Protection Policy and the Data Protection Legislation;]

any device personally belonging to an employee and personal data shall not be transferred to devices belonging to agents, contractors or other third parties working on behalf of the Company where the party in question does not comply fully with the Company's Data Protection Policy and the Data Protection Legislation;]

- p) All personal data stored on the Company's systems shall be backed up <<insert interval>> [e.g. daily] to an offsite location. All backups should be encrypted;

and be backed up <<insert interval>> [e.g. daily] to an offsite location. All backups should be encrypted;

- q) All electronic copies of personal data should be stored securely using strong passwords and encryption;

should be stored securely using strong passwords and encryption;

- r) All passwords used to access the Company's systems should be changed regularly and should be stored securely;

should be changed regularly and should be stored securely;

- s) Under no circumstances should passwords be written down or shared. If a password is forgotten, it should be reset using the applicable method. IT staff do not have access to passwords;

passwords be written down or shared. If a password is forgotten, it should be reset using the applicable method. IT staff do not have access to passwords;

- t) All software should be kept up to date. Security-related updates should be installed [not more than 30 days] OR [as soon as reasonably possible after] becoming available;

security-related updates should be installed [not more than 30 days] OR [as soon as reasonably possible after] becoming available;

- u) No software may be installed on a Company-owned computer or device without approval; and

Company-owned computer or device without approval; and

- v) 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 individuals who have opted out, whether directly or via a third-party service provider;

is used for marketing purposes, it shall be the responsibility of the Company to ensure that the appropriate consent is obtained from individuals who have opted out, whether directly or via a third-party service provider;

5.2 The following organisational measures shall be in place within the Company to protect the security of personal data: refer to Part 27 of the Company's Data Protection Policy

in place within the Company to protect the security of personal data: refer to Part 27 of the Company's Data Protection Policy

- a) All employees and contractors shall be made fully aware of their responsibilities under the Company's Data Protection Policy and the Data Protection Legislation and under the Company's Data Protection Policy;

on behalf of the Company shall be made fully aware of their responsibilities under the Data Protection Legislation and under the Company's Data Protection Policy;

- b) Only employees and contractors who need access to, and are authorised to, have access to personal data shall be given access to personal data;

on behalf of the Company that need access to, and are authorised to, have access to personal data;

- c) All employees and contractors handling personal data will be made aware of their responsibilities under the Company's Data Protection Policy and the Data Protection Legislation;

on behalf of the Company handling personal data will be made aware of their responsibilities under the Company's Data Protection Policy and the Data Protection Legislation;

- d) All employees and contractors handling personal data will be made aware of their responsibilities under the Company's Data Protection Policy and the Data Protection Legislation;

on behalf of the Company handling personal data will be made aware of their responsibilities under the Company's Data Protection Policy and the Data Protection Legislation;

- e) All employees and contractors handling personal data should exercise caution when discussing any work relating to personal data;

on behalf of the Company handling personal data should exercise caution when discussing any work relating to personal data;

- f) Methods of collecting, storing and processing personal data shall be regularly evaluated and reviewed;

ing personal data shall be regularly evaluated and reviewed;

A

M

P

L

E

S

- g) The performance of other parties working on behalf of the Company shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of the Company handling personal data will be required to comply with the Data Protection Legislation and the Company's Data Protection Policy;
- i) All agents, contractors and other parties working on behalf of the Company handling personal data shall be held to the same standards as relevant employees of the Company arising out of the Data Protection Legislation and the Company's Data Protection Policy;
- j) Where any agent, contractor or other party working on behalf of the Company handles personal data in breach of the Data Protection Legislation and/or the Company's Data Protection Policy, that party shall indemnify and hold the Company harmless against any costs, liability, damages, loss, claims or expenses that may arise out of that failure.

A

6. Data Disposal

Upon the expiry of the data retention period set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed or otherwise disposed of as follows:

- 6.1 Personal data stored on physical media (including any and all backups thereof) shall be deleted [see <<insert description of method of deletion>> method];
- 6.2 [Special category personal data] shall be deleted electronically (including any and all backups thereof) solely using the <<insert method of deletion>> method];
- 6.3 Personal data stored on physical media shall be shredded [to at least <<insert description of shredding level or standard>> method];
- 6.4 [Special category personal data] shall be shredded [to at least <<insert description of shredding level or standard>> method] OR [to be recycled] OR [<<insert description of final disposal method>>];

M

P

7. Data Retention

- 7.1 As stated above, the Company shall not retain any personal data for a longer period than is necessary in light of the purpose(s) for which that data is collected.
- 7.2 Different types of personal data, for different purposes, will necessarily be retained for different periods (which shall be periodically reviewed), as set out below.
- 7.3 When establishing retention periods, the following shall be taken into account:
  - a) The objectives and purposes for which the personal data is collected;
  - b) The type of personal data collected;
  - c) The purpose(s) for which the personal data is collected, held, and processed;

L

E

- d) The Company's legal basis for collecting, storing, and processing that data;
  - e) The category or categories of data to whom the data relates;
  - f) <<Insert additional criteria for retention of data>>.
- 7.4 If a precise retention period is not defined for a particular type of data, the retention of the data will be determined, thereby resolving any question, and the retention of that data, can be determined on the basis of those criteria.
- 7.5 Notwithstanding the retention periods, certain personal data may be deleted or destroyed prior to the expiry of its defined retention period where it is necessary for the Company to do so (whether in response to a request from the data subject or otherwise).
- 7.6 [In limited circumstances, it may be necessary to retain personal data for longer periods where it is necessary for archiving purposes that are in the public interest, for research purposes, or for statistical purposes. All such retention is subject to the implementation of appropriate technical and organizational measures to protect the rights and freedoms of data subjects in accordance with the Data Protection Legislation.]

S

A

M

P

L

E



S

8. Roles and Responsibilities

8.1 The Company's Data Protection Officer, <<insert name of data protection officer>>, <<insert details of role>>

<<insert name of data protection officer>>

8.2 The Data Protection Officer is responsible for overseeing the implementation of this Policy, ensuring compliance with this Policy, and the Company's other data protection policies (including, but not limited to, its Data Protection Policy) in accordance with the Data Protection Legislation.

responsible for overseeing the implementation of this Policy, ensuring compliance with this Policy, and the Company's other data protection policies (including, but not limited to, its Data Protection Policy) in accordance with the Data Protection Legislation.

8.3 [The Data Protection Officer, <<insert details of responsible parties, e.g. department heads>>] <<insert details of role>> responsible for ensuring compliance with the above data protection policies throughout the Company] OR [within <<insert details of scope, e.g. "their departments">>].

[The Data Protection Officer, <<insert details of responsible parties, e.g. department heads>>] <<insert details of role>> responsible for ensuring compliance with the above data protection policies throughout the Company] OR [within <<insert details of scope, e.g. "their departments">>].

8.4 Any questions regarding the retention of personal data, or any other aspect of Data Protection, should be referred to the Data Protection Officer.

Any questions regarding the retention of personal data, or any other aspect of Data Protection, should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed to have been implemented on <<insert date>>. No part of this Policy shall have retroactive effect on or after this date.

<<insert date>>. No part of this Policy shall have retroactive effect on or after <<insert date>>.

This Policy has been approved and signed by:

**Name:** <<insert name>>

**Position:** <<insert position>>

**Date:** <<insert date>>

**Due for Review by:** <<insert name>>

**Signature:**

A

M

P

L

E