

<

D

>

y

1. Introduction

This Policy sets out the Company's approach to the collection, use, storage, and disposal of personal data of individuals (staff, customers, business contacts etc.) registered in <<insert company registration number>>, within the Company's jurisdiction (the "Company") regarding data protection and the privacy of personal data subject, e.g. staff, customers, business contacts 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 retained EU law version of the General Data Protection Regulation (the "UK GDPR"), as it forms part of the law in Northern Ireland by virtue of the Data Protection Act 2018 and the Data Protection Regulations 2003 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 working from home.

2. Definitions

"consent"

Company name>>, a company registered in <<insert company registration number>>, with its principal place of business at <<insert address>> ("the Company"). The rights of <<insert type(s) of data subject>> ("data subjects") in respect of their personal data under the "Data Protection Law" means all legislation and regulations including, but not limited to, the General Data Protection Regulation ((EU) 2016/679) and the Data Protection Act 2018, and the Data Protection Regulations 2003 as amended, and the European Union (Withdrawal) Act 2018, and the Electronic Communications Regulations 2003.

Regarding the collection, processing, 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 of the Company, including when working from home.

"data controller"

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 processor"

a natural or legal person or entity, 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 subject"

a natural or legal person or entity, which processes personal data on behalf of a data controller; living, identified, or identifiable person about whom the Company holds personal data;

“EEA”

“personal data”

“personal data breach”

“processing”

“pseudonymisation”

“special category personal data”

3. Scope

- 3.1 The Company shall comply with the spirit of the law in the handling of all personal data of all individuals with whom it interacts.
- 3.2 The Company shall ensure the highest standards of particular, home working, and safeguarding of its employees, agents, contractors, or other parties. This is vitally important to the Company.

S

A

M

P

L

E

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

any information relating to a data subject who 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 any other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;

a 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, disclosure by transmission, dissemination or otherwise making available, alignment or correction, restriction, erasure or destruction;

the 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 is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable person; and

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

to the letter of the law, but also to the spirit of the law, and the importance of the correct, lawful, and fair handling of personal data, and the legal rights, privacy, and trust of individuals.

flexible working arrangements and, in particular, home working, in providing a better work life balance for its employees, agents, contractors, or other parties. While working from home, it remains committed to protecting personal data and the rights and

STAMPED

- privacy of individual /.
- 3.3 The Company's Data Protection Officer, <<insert name of data protection officer>>, <<insert name of data protection officer>> is responsible for administering the Data Protection Officer is responsible for developing and implementing any applicable relevant policies and/or guidelines.
- 3.4 All <<insert applicable roles>> managers, department heads, supervisors etc.>> ensuring that all employees, agents, contractors, or other staff, on behalf of the Company comply with this Policy and, where necessary, implement such practices, processes, controls, and training measures, as may be necessary to ensure such compliance. Where appropriate, such measures and, in particular, training, shall be applied remotely to home workers.
- 3.5 Any questions relating to the Data Protection Law should be referred to the Data Protection Officer should always be referred to the Data Protection Officer in particular, the Data Protection Officer should always be referred to the Data Protection Officer in the following cases:
- a) if there is any question as to the lawful basis on which personal data is to be processed;
 - b) if consent is sought for the collection, hold, and/or process of personal data;
 - c) if there is any question as to the retention period for any particular type of data;
 - d) if any new notices or similar privacy-related documentation is required;
 - e) if any assistance is required in dealing with the exercise of a data subject's right of access, rectification, or deletion;
 - f) if a personal data breach (whether or actual) has occurred;
 - g) if there is any question as to security measures (whether technical or organisational) to protect personal data;
 - h) if there are any questions relating to the implementation and maintenance of a home working environment;
 - i) if personal data is transferred to third parties (whether such third parties are acting as data controllers or data processors);
 - j) if personal data is transferred outside of the UK and there are any questions as to how to do so;
 - k) when any significant change in processing activity is to be carried out, or when there is a significant change to existing processing activities, which will require a Data Protection Impact Assessment;
 - l) when personal data is used for purposes different to those for which it was originally collected;
 - m) if any automated profiling or automated decision-making, is to be implemented;
 - n) if any assistance is required in complying with the law applicable to direct marketing.

S

4. The Data Protection Principles

This Policy aims to ensure compliance with the Data Protection Law. The UK GDPR sets out the following principles. Data controllers are responsible for ensuring compliance. All personal data

must comply with the Data Protection Law. The UK GDPR sets out the following principles. Data controllers are responsible for ensuring compliance. All personal data

4.1 processed lawfully, in relation to the data subject;

in a lawful 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 processing for archiving in the public interest, scientific or historical research purposes shall not be considered to be incompatible with those purposes;

collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing for archiving in the public interest, scientific or historical research purposes shall not be considered to be incompatible with those purposes;

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

adequate, relevant and limited to what is necessary in relation to the purposes for which the data is 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 is processed, or rectified without delay;

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 is 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 identification of data subjects for as long as the personal data will be used for the purposes of the public interest, scientific or historical research purposes, subject to implementation of appropriate technical and organisational measures required by the UK GDPR in order to safeguard the freedoms of the data subject;

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 identification of data subjects for as long as the personal data will be used for the purposes of the public interest, scientific or historical research purposes, subject to implementation of appropriate technical and organisational measures required by the UK GDPR in order to safeguard the 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;

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 of data subjects:

The UK GDPR sets out the rights of 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');

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.

automated decision making and profiling.

6. Lawful, Fair, and Transparent

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

personal data is processed lawfully, fairly, and transparently to the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following conditions is met:

A

M

P

L

E

S

- 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;
- 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 the purposes of the legitimate interests pursued by the controller or 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 considered as “sensitive personal data” and if 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 them from doing so);
- b) the processing is necessary for the purpose of carrying out the obligations and exercising the rights of the data controller or of the data subject in connection with employment, social security, and social protection law (provided by law);
- c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is 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 purpose of its legitimate activities, provided that the data is processed solely to the members or former members or persons who have regular contact with it in connection with those activities and that the personal data is not disclosed outside the association or other body;
- 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 for 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 to safeguard 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

A

M

P

L

E

S

A

M

P

L

E

an employee
care or treat
or services o
professional
Data Protect

for the provision of health or social
nt of health or social care systems
rsuant to a contract with a health
ditions and safeguards set out in

i) the process
public health
threats to h
health care a
of law which
the rights an
secrecy); or

lic interest reasons in the area of
ing against serious cross-border
standards of quality and safety of
s or medical devices, on the basis
d specific measures to safeguard
subject (in particular, professional

j) the process
interest, so
purposes wi
pursued, re
provide for
fundamental

archiving purposes in the public
research purposes, or statistical
shall be proportionate to the aim
the right to data protection, and
c measures to safeguard the
of the data subject.]

7. Consent

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

collecting, holding, and/or processing

7.1 Consent is a clear, affirmative statement or action by the data subject that they agree to the processing of their personal data. It cannot be inferred from silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

a subject that they agree to the
ear indication may take the form of
ore-ticked boxes, or inactivity are

7.2 Where consent is one of the lawful bases for processing, it must be freely given, specific, informed, and unambiguous. It must be distinguished from other matters.

which includes other matters, the
clearly separate from such other

7.3 Data subjects are free to withdraw their consent at any time and it must be made easy for them to do so. Any withdrawal of consent must be honoured promptly.

at any time and it must be made
draws consent, their request must

7.4 If personal data is to be processed for a purpose that is incompatible with the purpose for which it was originally collected that was disclosed to the data subject when they first provided their consent, consent cannot be relied upon. New or different purposes may need to be obtained from the data subject.

erent purpose that is incompatible
that personal data was originally
a subject when they first provided
e or purposes may need to be

7.5 [If special category data is to be processed, the Company shall normally rely on a lawful basis other than consent. If explicit consent is relied upon, the data subject must be given clear notice in order to consent.]

ssed, the Company shall normally
nsent. If explicit consent is relied
be issued with a suitable privacy

7.6 In all cases where consent is the lawful basis for processing, records must be kept of all consents obtained in order to demonstrate compliance with consent requirements.

as the lawful basis for collecting,
ords must be kept of all consents
y can demonstrate its compliance

8. Specified, Explicit, and Legitimate

8.1 The Company collects and processes personal data set out in Part 24 of

personal data set out in Part 24 of

S

this Policy. This includes

a) personal data

data subjects[.] OR [; and]

b) [personal data

ties.]

8.2 The Company only
specific purposes
expressly permitted

and holds personal data for the
this Policy (or for other purposes

8.3 Data subjects must
for which the Company
more information on

times of the purpose or purposes
data. Please refer to Part 15 for
informed.

9. Adequate, Relevant, and

g

9.1 The Company will
necessary for the
been informed (or v
Part 24, below.

personal data for and to the extent
poses of which data subjects have
er Part 8, above, and as set out in

9.2 Employees, agents
Company may collect
performance of the
Excessive personal

parties working on behalf of the
y to the extent required for the
in accordance with this Policy.
ed.

9.3 Employees, agents
Company may process
duties requires it. P
for any unrelated re

parties working on behalf of the
when the performance of their job
the Company cannot be processed

10. Accuracy of Data and Key

10.1 The Company shall
held by it is kept ac
the rectification of p
Part 17, below.

al data collected, processed, and
This includes, but is not limited to,
est of a data subject, as set out in

10.2 The accuracy of pe
[regular] OR [<<ins
found to be inaccur
without delay to am

checked when it is collected and at
thereafter. If any personal data is
reasonable steps will be taken
s appropriate.

11. Data Retention

11.1 The Company shall
light of the purpose
collected, held, and

for any longer than is necessary in
that personal data was originally

11.2 When personal data
erase or otherwise
27 of this Policy (in
and in our Data Ret

l reasonable steps will be taken to
y. Further detail is provided in Part
personal data for home workers)

11.3 For full details of
retention periods fo
refer to our Data Re

ach to data retention, including
types held by the Company, please

A

M

P

L

E

12. Secure Processing

- 12.1 The Company shall ensure that personal data collected, held, and processed is kept secure against unauthorised or unlawful access, destruction, or damage. Further measures which shall be taken are provided in Parts 25 and 26.
- 12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed to ensure their ongoing effectiveness and the continued security of the data.
- 12.3 Data security must be achieved by protecting the confidentiality, integrity, and availability of the data as follows:
- a) only those who have a valid business need to access and use personal data and who are authorised to do so shall access and use it;
 - b) personal data shall be stored in a secure and suitable for the purpose or purposes for which it is collected, held, and processed; and
 - c) authorised users shall be able to access the personal data as required for the purpose or purposes.

13. Accountability and Records

- 13.1 The Data Protection Officer shall be responsible for administering this Policy and for developing and implementing related policies, procedures, and/or guidelines.
- 13.2 The Company shall adopt a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted where processing presents a significant risk to the rights and freedoms of individuals (please refer to Part 14 for further information).
- 13.3 All employees, agents, and other parties working on behalf of the Company shall be trained in data protection and privacy, including the Data Protection Law, this Policy, and all other applicable Company policies.
- 13.4 The Company's data protection measures shall be regularly reviewed and updated as necessary.
- 13.5 The Company shall maintain accurate records of all personal data collection, holding, and processing. These records shall incorporate the following information:
- a) the name and contact details of the Company, its Data Protection Officer, and any applicable data processors (including data processors and other data controllers to whom personal data is shared);
 - b) the purpose for which the personal data is collected, held, and processed;
 - c) the Company's legal basis for processing such consent, the records of such consent, and the records of the collection and processing of personal data;
 - d) details of the personal data collected, held, and processed, including the categories of data subject to processing.

S

- e) details of any transfers of personal data to non-UK countries including the legal basis for such transfers;
- f) details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);
- g) details of personal data storage location(s);
- h) detailed description of technical and organisational measures implemented to ensure the security of personal data.

14. Data Protection Impact Assessment

Privacy by Design

- 14.1 In accordance with the Data Protection 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 by design 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 of the collection, holding, and processing;
 - b) the state of the art and the measures to be taken to protect personal data;
 - c) the cost of implementing measures;
 - d) the risks posed to the Company, 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 personal data is to be used;
 - c) the Company's legal basis for processing;
 - d) how personal data will be stored and protected;
 - 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 following is 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 of the following at the time of collection; and

A

M

P

L

E

E

- | | |
|------|--|
| 15.2 | The following information shall be provided to the data subject in the form of a privacy notice: |
| a) | details of the personal data being collected, not limited to, contact details, and the names and contact details of the 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 purpose(s) of this Policy) and the lawful basis justifying the processing; |
| c) | where applicable, the legal interests upon which the Company is relying in the processing of 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 the third parties; |
| f) | where the personal data is transferred to a third party that is located outside the EEA, details of that transfer, including but not limited to the measures in place to ensure Part 31 of this Policy for further details); |
| g) | details of applicable retention periods; |
| h) | details of the rights of the data subject under Data Protection Law; |
| i) | details of the right of the data subject to withdraw their consent to the processing of their personal data at any time; |
| j) | details of the right of the data subject to complain to the Information Commissioner; |
| k) | where the personal data is obtained directly from the data subject, details about the source of the personal 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 logic involved in those decisions, and any consequences of those decisions; |

16.1 Data subjects may request (“SARs”) at any time to find out more about the Company holds about them, what it is doing with that

E

- © Simply-Docs – BS.DAT.08 Home Working Data 11

E

- 18.4 All employees, age 16 or over, who are working for parties working on behalf of the Company working for the Company must ensure that all personal data that they are working with is kept secure and, wherever possible, only stored [and processed] within the system(s) and name(s) and/or description(s) of system(s)>>] system(s) and must cooperate in ensuring that any personal data held by them at home is erased within the time limit.

19.3 All employees, agents or parties working on behalf of the Company working for the Company shall ensure that all personal data that they are working with is kept secure and, wherever possible, only stored [and processed] within the system(s) and/or description(s) of system(s)>>] systems. The rapid and/or centralised application of restrictions shall fully with the Company's Data

Protection Officer in
not processed further
computers or device

onal data held by them at home is
appropriate, erasing such data from

20. **[Data Portability]**

- 20.1 The Company pro using automated means. <<Insert details of automated
- 20.2 Where data subject consent to the Company to process their personal data in su processing is otherwise required for the performance of the Company and the data subject, data subjects have protection Law, to receive a copy of their personal data purposes (namely transmitting it to other data controller
- 20.3 To facilitate the right Company shall make available all applicable personal the following format[s]:
- a) <<list format
- b) <<add further
- 20.4 Where technically f a data subject, personal data shall be sent directly to th r.
- 20.5 All requests for co shall be complied with within one month of the data s period can be extended by up to two months in the case requests. If such additional time is required, the data s

21. **Objections to Personal D**

- 21.1 Data subjects hav to the Company processing their personal data base s, for direct marketing (including profiling), [and proc or historical research and statistics purposes].
- 21.2 Where a data subje any processing their personal data based on its legitim any shall cease such processing immediately, unless ed that the Company's legitimate grounds for such p data subject's interests, rights, and freedoms, or that th y for the conduct of legal claims.
- 21.3 Where a data subje any processing their personal data for direct marketin any shall cease such processing promptly.
- 21.4 [Where a data subj any processing their personal data for scientific and/o nd statistics purposes, the data subject must, under demonstate grounds relating to his or her particular si is not required to comply if the research is necessa of a task carried out for reasons of public interest.]

22. **[Automated Processing, a**

- 22.1 [The Company use making, and Profiling automated decision-making processes

- as follows:
- a) <<Insert details of the decision-making>>.]
 - 22.2 [The Company uses the following purposes as follows:
 - a) <<Insert details of the purposes>>.]
 - 22.3 The activities described in this Policy are generally prohibited under Data Protection Law where the activities have a legal or similarly significant effect on the data subject if one of the following applies:
 - a) the data subject has not given explicit consent;
 - b) the processing is necessary for the performance of a contract entered into by the data subject;
 - c) the processing is necessary for the entry into, or performance of, a contract between the data subject and the Company.
 - 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; or
 - b) the processing is necessary for reasons of substantial public interest.
 - 22.5 Where decisions are made using automated processing (including profiling), data subjects have the right to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation of the logic involved. Data subjects must be explicitly informed of this right at the point of contact.
 - 22.6 In addition to the above, data subjects must be provided to data subjects explaining 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 safeguards shall be used;
 - b) technical and organisational measures shall be implemented to ensure that the data is secure, such measures must enable the data subject to be able to access their data;
 - c) all personal data processed in this manner shall be secured in accordance with the requirements of the Data Protection Act (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 the relevant 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 provided that the customer's contact details have been obtained in a lawful manner and the marketing relates to similar products or services to those which the customer in question has been given the

- opportunity
collected and
- 23.3 The right to object shall be explicitly offered to data subjects in a clear and concise manner and must be kept separate from other information in the privacy policy.
- 23.4 If a data subject objects, their request must be complied with promptly. A list of circumstances to ensure that the data subject's marketing preferences are respected with.]

24. **Personal Data Collected,**

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

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

25. **Data Security - Transferring**

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

- 25.1 All emails containing personal data shall be encrypted [using <<insert type(s) of encryption>>];
- 25.2 Employees, agents or third parties working on behalf of the Company working from home [should, whenever possible and practical,] only access personal data when connected to the Company's Virtual Private Network (VPN).
- 25.3 All emails containing personal data shall be marked "confidential";
- 25.4 Personal data may only be transmitted over secure networks only; transmission over unsecured networks shall not be permitted in any circumstances. All employees, agents or third parties working on behalf of the Company working from home shall ensure that their home network is secure and, where reasonably possible, any and all personal data shall be transmitted using secure network equipment such as modems and routers are installed and security software or firewalls are installed and assistance is available from the Company.

g when their details were first collected and communication from the Company.

shall be explicitly offered to data subjects in a clear and concise manner and must be kept separate from other information in the privacy policy.

g, their request must be complied with promptly. A list of circumstances to ensure that the data subject's marketing preferences are respected with.]

d processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

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

Communications

asures are taken with respect to all communications and other personal data:

- encrypted [using <<insert type(s) of encryption>>];
- parties working on behalf of the Company working from home [should, whenever possible and practical,] only access personal data when connected to the Company's Virtual Private Network (VPN).
- marked "confidential";
- secure networks only; transmission over unsecured networks shall not be permitted in any circumstances. All employees, agents or third parties working on behalf of the Company working from home shall ensure that their home network is secure and, where reasonably possible, any and all personal data shall be transmitted using secure network equipment such as modems and routers are installed and security software or firewalls are installed and assistance is available from the Company.

E

insert name of data protection
D/OR [IT Department, <<insert
s), position(s), department(s), and

- er a wireless network if there is a
le;
email, whether sent or received,
ail and stored securely. The email
associated therewith should also
n>>];
ssimile transmission the recipient
mission and should be waiting by
hardcopy form it should be passed
insert name(s) and/or type(s) of
be transferred to home workers in
stances.];
y, whether in hardcopy form or on
red in a suitable container marked
d>>.]

The Company shall ensure storage of personal data:

ures are taken with respect to the

- should be stored securely using [redacted] data encryption;
- any electronic copies stored on [redacted] securely in a locked box, drawer, [redacted] shall provide suitable storage [redacted]ees, agents, contractors, or other [redacted]working from home who are likely to [redacted]
- and be backed up <<insert interval>> [redacted] backup system>> with backups [redacted]ups should be encrypted [using [redacted]
- ices (including, but not limited to, [redacted]her such device belongs to the [redacted]to the extent absolutely necessary [redacted]Furthermore, employees, agents, [redacted]half of the Company working from [redacted]le and practical] only access and [redacted]to the Company's Virtual Private [redacted]
- o, stored on, accessed from, or [redacted]nging to employees [with the [redacted]ection Officer, only] to the extent [redacted]

S

A

M

P



F

or parties working on behalf of the
that they use all reasonable efforts

S

A

M

P

L

E

to comply with Part 2 of the Data Protection Act 1998, by ensuring that a specific room or part of a building is reserved for the storage of data with lockable windows and doors, particularly when handling personal data. The Company shall ensure a degree of security that is reasonably practical in the circumstances.

28.6 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, either directly or via a third-party service.

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

including, for example, setting aside a specific room or part of a building behind a lockable door, in a room reserved for the storage of data, particularly when handling personal data. Workers may not always be able to access the Company's premises, but all measures shall be made to ensure the best security possible in the circumstances.

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

>>].

29. Data Security - IT Security

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

29.1 All passwords used for access to IT systems should be changed regularly and should not use words or phrases that can 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.

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

29.3 All software (including applications and operating systems) installed on IT equipment should be kept up-to-date. Updates should be made as soon as possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so.

29.4 All software (including applications and operating systems) installed on IT equipment belonging to employees, agents, contractors, or other parties working on behalf of the Company should be kept up-to-date. Updates should be made as soon as possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so. Updates should be made automatically where possible, or by IT staff in order to ensure that all equipment is up-to-date. Automatic updates should be made where possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so. Advice should be sought from the Company's [Data Protection Officer, <<insert name of Data Protection Officer>>], <<insert contact details>>] AND/OR [IT Department, <<insert name(s), position(s)>>] AND/OR [<<insert contact details>>] AND/OR [<<insert contact details as required>>].

29.5 No software may be installed on a company-owned computer or device without the prior approval of the Company. Updates should be made as soon as possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so.

measures are taken with respect to IT and information security:

should be changed regularly and should not use words or phrases that can 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.

words be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company. If a password is forgotten, it must be changed using a secure method. IT staff do not have access to passwords.

applications and operating systems) installed on IT equipment should be kept up-to-date. Updates should be made as soon as possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so.

applications and operating systems) installed on IT equipment belonging to employees, agents, contractors, or other parties working on behalf of the Company should be kept up-to-date. Updates should be made as soon as possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so. Updates should be made automatically where possible, or by IT staff in order to ensure that all equipment is up-to-date. Automatic updates should be made where possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so. Advice should be sought from the Company's [Data Protection Officer, <<insert name of Data Protection Officer>>], <<insert contact details>>] AND/OR [IT Department, <<insert name(s), position(s)>>] AND/OR [<<insert contact details>>] AND/OR [<<insert contact details as required>>].

company-owned computer or device without the prior approval of the Company. Updates should be made as soon as possible, but no later than <<insert period>> after the release of a new version or manufacturer's update, unless there are valid technical reasons for not doing so.

S

29.6 All employees, agents, contractors, or other parties working on behalf of the Company working with personal data on IT equipment shall be given advice on the installation of new devices from the [IT Department, <<insert contact details>>] before installing such software; [<<insert name(s), position(s), department(s), and required>>]

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

30. Organisational Measures

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

30.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made aware 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 access 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 in accordance with the information provided to the data subjects. 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 (including those working from home) will be required to follow the appropriate security methods;

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 Data Retention Policy;

30.9 The performance of agents, contractors, or other parties working on behalf of the Company in 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 Company's 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 handling of personal data are held to the same conditions as those set out in the Company's Policy and Data Protection Policy arising out of this

A

M

P

L

E

30.12 Where any agent, contractor or other party working on behalf of the Company handles or handles or handles personal data in connection with the Company's business, the Company shall indemnify and hold the Company harmless from and against all costs, damages, loss, claims and expenses (including reasonable legal fees) that may arise out of that failure;

30.13 [<<Add further organisational measures as required>>.]

31. Transferring Personal Data Outside the UK

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

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

- The UK has made an adequacy decision (referred to as 'adequacy decision') in relation to the country in question. From 1 January 2021, transfers of personal data to EEA countries will continue to be permitted. The UK will also be in place to recognise pre-existing EU adequacy decisions.
- Appropriate safeguards are in place, including binding corporate rules, approved for use in the UK (this includes those adopted by the Information Commissioner prior to 1 January 2021), or an approved certification mechanism.
- The transfer is made on the basis of informed and explicit consent of the data subject.
- The transfer is necessary for the performance of a contract between the data subject and the Company, for the protection of public interest reasons; for the establishment or defence of legal claims; to protect the vital interests of the data subject; or, in limited circumstances, for the benefit of the data subject.

32. Data Breach Notification

32.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer. Personal data breaches which relate to the Company's business, including those involving employees, agents, contractors, or other parties working on behalf of the Company, whether from home, using either personal or Company computers or devices, must be reported.

32.2 If an employee, agent, contractor or other party working on behalf of the Company becomes aware that a personal data breach has occurred, they must report it to the Data Protection Officer. Any and all evidence relating to the breach must be 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, disclosure of sensitive information, or other significant social or economic damage), the Data Protection Officer must ensure that the

- Information Commissioner and in any event, within 72 hours of becoming aware of the breach without delay, and in any event, within 72 hours of becoming aware of it.
- 32.4 In the event that a breach is likely to result in a high risk (that is, a higher risk than that referred to in 32.3) to the rights and freedoms of data subjects, the Company must ensure that all affected data subjects are informed and without undue delay.
- 32.5 Data breach notification must include the following information:
- 32.5.1 The category of data subjects concerned;
- 32.5.2 The category of personal data records concerned;
- 32.5.3 The name and contact details of the Company's Data Protection Officer (or other contact point where information can be obtained);
- 32.5.4 The likely consequences of the breach;
- 32.5.5 Details of the measures proposed to be taken, by the Company to mitigate or eliminate the adverse effects.
33. **Implementation of Policy**
- This Policy shall be deemed to have been implemented on the date of its adoption. No part of this Policy shall have retroactive effect prior to this date.

This Policy has been approved and signed by:

Name: <<insert name>>

Position: <<insert position>>

Date: <<insert date>>

Due for Review by: <<insert date>>

Signature: