

## 1. Introduction

This Policy sets out the Company's policy regarding data protection, registered in <<insert company registration number>>, with the <<insert company name>> ("the Company") regarding data protection ("employee data subjects") under the Data Protection Law. "Data Protection Law" means the law regulating the use of personal data, including, but not limited to, the Data Protection Regulation ((EU) 2016/679) in England and Wales, Scotland, and the European Union (Withdrawal) Act 2018 and Electronic Communications Act 2000 and any successor legislation.

This Policy sets out the Company's policy regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out in this Policy must be followed at all times by the Company, its employees, and any other parties working on behalf of the Company.

## 2. Definitions

**"consent"**

<<insert company name>>, a company registered in <<insert company registration number>>, with the <<insert company name>> ("the Company") is at <<insert address>> ("the Company's address") of its employees (in this context, "employee data subjects") under Data Protection Law. "Data Protection Law" means the law regulating the use of personal data, including, but not limited to, the Data Protection Regulation ((EU) 2016/679) in England and Wales, Scotland, and the European Union (Withdrawal) Act 2018 and Electronic Communications Act 2000 and any successor legislation.

This Policy sets out the Company's policy regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out in this Policy must be followed at all times by the Company, its employees, and any other parties working on behalf of the Company.

**"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 employee data subjects;

**"data subject"**

a natural or legal person or entity, which processes personal data on behalf of a data controller;

any living, identified, or identifiable person about whom the Company processes personal data (in this context, employee data subjects);

A  
M  
P  
L  
E



“EEA”

“personal data”

“personal data breach”

“processing”

“pseudonymisation”

“special category personal data”

### 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 is <<insert name of data protection officer>>, <<insert name of Data Protection Officer is responsible for the day-to-day responsible [, work in the HR Department, or position of the Data Protection Officer].>>

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 one or more 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 combination, 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 are in place to 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, and data concerning health, sexual life, sexual orientation, and genetic data.

not only to the letter of the law, but also to the spirit of the law, and to ensure the correct, lawful, and fair handling of all personal data, and to ensure the legal rights, privacy, and trust of all individuals with whom we do business.

<<insert name of data protection officer>> is the Data Protection Officer responsible for the day-to-day administration of this Policy and is responsible for administering this Policy and for ensuring that the Company complies with the requirements of the GDPR.



S

for developing and  
and/or guidelines.

able related policies, procedures,

- 3.3 All <<insert appl  
supervisors etc.>>  
contractors, or othe  
this Policy and, whe  
controls, and trai  
compliance.

managers, department heads,  
ensuring that all employees, agents,  
half of the Company comply with  
ement such practices, processes,  
ply necessary to ensure such

- 3.4 Any questions rela  
referred to the Da  
Officer should alway

Data Protection Law should be  
n particular, the Data Protection  
following cases:

- a) if there is  
employee pe
- b) if consent is  
employee pe
- c) if there is a  
particular typ
- d) if any new  
documentati
- e) if any assis  
employee o  
handling of s
- f) if a personal
- g) if there is  
technical or  
data;
- h) if employee  
such third pa
- i) if employee  
there are qu
- j) when any s  
significant c  
which will re
- k) when emplo  
those for wh
- l) if any autom  
making, is to
- m) if any assis  
direct marke

g to the lawful basis on which  
ected, held, and/or processed;

order to collect, hold, and process

to the retention period for any  
al data;

notices or similar privacy-related

dealing with the exercise of an  
cluding, but not limited to, the

or actual) has occurred;

to security measures (whether  
d to protect employee personal

shared with third parties (whether  
controllers or data processors);

transferred outside of the UK and  
al basis on which to do so;

g activity is to be carried out, or  
e to existing processing activities,  
mpact Assessment;

be used for purposes different to  
ected;

g profiling or automated decision-

plying with the law applicable to

#### 4. The Data Protection Princ

This Policy aims to ensure  
out the following principles  
Data controllers are resp  
compliance. All personal da

rotection Law. The UK GDPR sets  
dling personal data must comply.  
be able to demonstrate, such

- 4.1 processed lawfully,

ent manner in relation to the data

A

M

P

L

E



# S

# A

# M

# P

# L

# E

subject;

4.2 collected for specific 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 the original purposes;

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 are 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 identification of data subjects for as long as the personal data will be processed solely for archiving in 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 that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

## 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 to or affecting the rights of the data subject. Specifically, personal data shall be lawful only 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 a data subject to enter into a contract;



S

- 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 data controller;
- f) the processing is necessary for the purposes of the legitimate interests pursued by the data 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 to be 'sensitive personal data' as defined in Article 9(1), the following conditions must be met in addition to one or more of the conditions set out above:

- 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 data controller from seeking such consent);
- 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, where the processing is authorised by law or a collective agreement 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 unable to give 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 course of its legitimate activities, provided that the data controller is not solely for the members or former members of the association or body who have regular contact with it in connection with its 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 of the data controller's judicial capacity;
- g) the processing is necessary for substantial public interest reasons, on the basis of which the data controller, on a proportionate to the aim pursued, shall implement appropriate 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 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

A

M

P

L

E



- professional and safeguards referred to in Article 9(3) of the GDPR
- i) the processing is necessary for reasons of public health, such as threats to health care or health care of law which the rights and freedoms of the subject (in particular, professional secrecy); or
  - j) the processing is necessary for reasons of public interest, such as research purposes, or statistical purposes in the public interest, as provided for in 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 of the subject, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the subject.

## 7. Consent

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

- 7.1 Consent is a clear and affirmative indication from a subject that they agree to the processing of their personal data. It may take the form of a statement or a pre-ticked box, or inactivity are unlikely to amount to consent.
- 7.2 Where consent is given in the context of a document 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 subject withdraws consent, their request must be honoured promptly.
- 7.4 If personal data is to be used for a purpose other than that for which it was originally collected that was not within the scope of their consent, consent must be obtained from the data subject.
- 7.5 Where special categories of personal data are processed, the Company shall 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 fully informed.
- 7.6 In all cases where consent is the lawful basis for collecting, holding, and/or processing personal data, the Company must keep records of all consents obtained in order to demonstrate its compliance with consent requirements.

## 8. Specified, Explicit, and Legitimate Interest

- 8.1 The Company collects and processes employee personal data set out in Parts 23 to 28 of this Policy.



- a) personal data subjects and] employee data subjects[.] OR [;
- b) [personal data subjects.] parties.]
- 8.2 The Company only holds employee personal data for the specific purposes set out to 28 of this Policy (or for other purposes expressly permitted by the Data Protection Law).
- 8.3 Employee data subjects are informed at all times of the purpose or purposes for which their personal data is held. Please refer to Part 15 for more information on how data subjects are informed.
9. **Adequate, Relevant, and Necessary**
- 9.1 The Company will only collect employee personal data for and to the extent necessary for the purposes of which employee data subjects have been informed) as under Part 8, above, and as set out in Part 15.
- 9.2 Employees, agents or other parties working on behalf of the Company may collect employee personal data only to the extent required for the performance of their duties and in accordance with this Policy. Excessive personal data will not be collected.
- 9.3 Employees, agents or other parties working on behalf of the Company may process employee personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any other purpose.
10. **Accuracy of Data and Keeping Data Up-to-date**
- 10.1 The Company shall ensure that employee personal data collected, processed, and held is accurate and up-to-date. This includes, but is not limited to, the requirement to update data at the request of an employee data subject, as set out in Part 15.
- 10.2 The accuracy of employee personal data shall be checked when it is collected and at [regular] OR [other specified] intervals thereafter. If any employee personal data is found to be out-of-date, all reasonable steps will be taken without delay to ensure that data, as appropriate.
- 10.3 It is the responsibility of the employee data subjects to ensure that the personal data they provide to the Company is kept up-to-date. If any employee data subject should ensure that the relevant personal data is updated as soon as is reasonably practicable. The Company will encourage its employees to help meet its obligations under the Law.
11. **Data Retention**
- 11.1 The Company shall not retain employee personal data for any longer than is necessary in light of the purposes for which it was originally collected, held, and processed.
- 11.2 When employee personal data is no longer required, all reasonable steps will be taken to erase or securely destroy the data securely and without delay.



- 11.3 For full details of retention periods for each type of employee personal data held by the Company, please refer to our Data Retention Policy.

## 12. Secure Processing

- 12.1 The Company shall ensure that employee personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful access, disclosure, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 29 and 30.
- 12.2 All technical and organisational measures shall be regularly reviewed to ensure their effectiveness and that they are appropriate to the risks to employee personal data.
- 12.3 Data security must be maintained by protecting the confidentiality, integrity, and availability of employee personal data as follows:
- a) only those who have a valid business need may access and use employee personal data and who have been authorised to do so;
  - b) employee personal data shall be stored securely and suitably for the purpose or purposes for which it is collected, held, and processed; and
  - c) authorised users shall be able to access employee personal data as required for the purpose or purposes.

## 13. Accountability and Records

- 13.1 The Data Protection Officer, or a senior responsible person, shall be responsible [ , working together with the relevant department or position, e.g. HR Manager>>], for administering and overseeing the development and implementing any applicable related policies, procedures, or guidelines.
- 13.2 The Company shall adopt a 'privacy by design' approach at all times when collecting, holding, or processing employee personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of employee data subjects (please refer to Part 14 for further details).
- 13.3 All employees, agents, contractors, and other parties working on behalf of the Company shall be responsible for ensuring compliance with data protection and privacy, including the Data Protection Law, this Policy, and all applicable regulations.
- 13.4 The Company's data protection measures shall be regularly reviewed and updated as necessary.
- 13.5 The Company shall maintain records of all employee personal data collection, holding, and processing activities which shall incorporate the following information:
- a) the name and contact details of the person responsible for the data, and any applicable laws, regulations, or other data collection requirements;
  - b) the purpose and lawful basis for the collection, holding, and processing of employee personal data;



- c) the Company shall obtain the consent of the employee (including, where applicable, obtaining such consent, and records of obtaining, and processing employee personal data);
- d) details of the personal data collected, held, and processed by the Company, and the categories of employee data subject to which the data relates;
- e) details of any transfer of personal data to non-UK countries and the safeguards;
- f) details of how long personal data will be retained by the Company (pursuant to the Company's Data Retention Policy);
- g) details of employee data storage, including location(s);
- h) detailed description of the technical and organisational measures taken by the Company to ensure the security of employee personal data.

#### 14. Data Protection Impact Assessment

- 14.1 In accordance with the principles of Data Protection by Design, for any and all new projects and/or processes which involve the use of new technologies and which are likely to result in a high risk to the rights and freedoms of individuals, the Company shall carry out a Data Protection Impact Assessment.
- 14.2 The principles of 'Data Protection by Design' shall be followed at all times when processing employee personal data. The following factors should be taken into account:
  - a) the nature, scope, and purpose of the collection, holding, and processing of the data;
  - b) the state of the art and the measures to be taken to protect the data;
  - c) the cost of implementing measures to protect the data;
  - d) the risks posed to the rights and freedoms of individuals, including the risks of discrimination, identity theft, and fraud.
- 14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
  - a) the type(s) of personal data that will be collected, held, and processed;
  - b) the purpose(s) for which the personal data is to be used;
  - c) the Company's policy on the use of the data;
  - d) how employee data will be used;
  - 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) for which the data is to be processed;
  - g) risks posed to the rights and freedoms of individuals;
  - h) risks posed to the Company; and



- i) proposed measures to 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 in relation to employee data subject to the Policy.

- a) Where employee personal data is collected directly from employee data subjects, the data subjects will be informed of its purpose at the time of collection;
- b) where employee personal data is obtained from a third party, the data subjects will be informed of its purpose:
  - i) if the data subject is to be contacted to communicate with the employee or to make a communication is made; or
  - ii) if the data subject is to be transferred to another party, before the transfer;
  - iii) as soon as possible and in any event not more than one month after the data is obtained.

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

- a) details of the identity of the Company, its contact details, and details of any representative or Data Protection Officer;
- b) the purpose for which the employee personal data is being collected and will be processed (see Parts 23 to 28 of this Policy) and the lawful basis for the collection, storage and processing;
- c) the interests upon which the Company is relying in relation to the employee personal data;
- d) where the employee personal data is not obtained directly from the data subject, the sources of personal data collected and processed;
- e) where the employee personal data is to be transferred to one or more third parties, the identity of those parties;
- f) where the employee personal data is to be transferred to a third party that is located outside the UK, details of that transfer, including but not limited to the legal basis for the transfer (see Part 36 of this Policy for further details);
- g) details of any retention periods;
- h) details of the data subject's rights under the UK GDPR;
- i) details of the data subject's right to withdraw their consent to the Company processing their personal data at any time (where applicable);
- j) details of the data subject's right to complain to the Information Commissioner;
- k) where the employee personal data is not obtained directly from the data subject, the source of that personal data;
- l) where applicable, details of any legal or contractual requirement or obligation relating to the collection, storage and processing of the employee



- personal data and the consequences of failing to provide it; and
- m) details of a decision made using automated processing, including information on how the decision was made, the logic involved in those decisions, and any consequences of those decisions.

## 16. Data Subject Access

- 16.1 Employee data subjects have the right to access requests ("SARs") at any time to find out more about the data which the Company holds about them, what it is doing with it, and why.
- 16.2 Employees wishing to exercise their right to access should do using a Subject Access Request Form, sent to the Company's Data Protection Officer at <<insert contact details>>.
- 16.3 Responses to SARs shall be made within one month of receipt; however, this may be extended to two months if the SAR is complex or numerous requests are received. In such additional time is required, the employee data subject shall be informed.
- 16.4 All SARs received shall be handled in accordance with the Company's Data Protection Officer Subject Access Request Policy and Procedure].
- 16.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has been provided to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repeated.

## 17. Rectification of Personal Data

- 17.1 Employee data subjects have the right to require the Company to rectify any of their personal data if it is inaccurate or incomplete.
- 17.2 The Company shall rectify the personal data in question, and inform the employee data subject of the rectification, within one month of the receipt of the request. The period can be extended by up to two months in the case of complex requests. If such an extension is required, the employee data subject shall be informed.
- 17.3 In the event that any personal data has been disclosed to third parties, those parties shall be notified of any rectification that must be made to that personal data.

## 18. Erasure of Personal Data

- 18.1 Employee data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
- a) it is no longer necessary for the Company to hold that employee's personal data for the purpose(s) for which it was originally collected or processed;



S

A

M

P

L

E

- b) the employee (where applicable) to withdraw their consent (where applicable) to the Company holding and processing their personal data;
- c) the employee to request the Company to stop processing their personal data where there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details on the right to object);
- d) the employee to request the Company to stop processing their personal data if it has been processed unlawfully;
- e) the employee to request the Company to stop processing their personal data so that it can be erased in order for the Company to comply with its legal obligation[;] **OR** [.]
- f) [the employee to request the Company to stop processing their personal data if it is being held and processed for the purpose of providing safety services to a child.]

18.2 Unless the Company is unable to do so, it shall endeavour to refuse to erase employee personal data, all of which shall be complied with, and the employee data subject shall be notified of the outcome, within one month of receipt of the request. The time period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be notified.

18.3 In the event that an employee data subject requests the erasure of personal data that is to be erased in response to a request, and the data has been disclosed to third parties, the Company shall endeavour to notify those parties shall be notified of the request (unless it is impossible or would require disproportionate effort).

## 19. Restriction of Personal Data

19.1 Employee data subject may, in certain circumstances, request that the Company ceases processing their personal data it holds about them. If an employee data subject requests the erasure of their personal data, the Company shall retain only the amount of employee data necessary for the purpose of the request concerning that data subject (if any) and shall ensure that the data in question is not processed further.

19.2 In the event that an employee data subject requests the erasure of their personal data has been disclosed to third parties, those parties shall be notified of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## 20. [Data Portability

20.1 The Company provides a service relating to employees using automated means. The service is provided using automated processing>>.

20.2 Where employee data subject requests the Company to stop processing their personal data, the Company shall endeavour to stop processing their personal data in a manner, or the processing is otherwise required by law, or the processing is necessary for a contract between the Company and the employee data subject, or the employee data subject has the right, under the UK GDPR, to request the Company to stop processing their personal data and to use it for other purposes (namely to provide a service to the employee data subject as a controller).

20.3 To facilitate the right of an employee data subject to request the Company to stop processing their personal data, the Company shall make available all employee data subjects in the following format[s]:

- a) <<list format>>



# S

- # A

# M

- P

## L

- E



- 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), employee data subjects must be provided with the right to object, to challenge such decisions, request human review, to express their own point of view, and to obtain an explanation from the Company. Employee data subjects must be given the right at the first point of contact.
- 22.6 In addition to the above, employee data subjects must be provided to employee data subjects explaining the basis of the decision-making or profiling, and the significance and consequences of the decision or decisions.
- 22.7 When employee personal data is subject to any form of automated processing, the following shall apply:
- a) appropriate legal procedures shall be used;
  - b) technical and organisational measures shall be implemented to minimise the risk of errors occurring, such measures must enable them to be effectively challenged;
  - c) all personal data shall be secured in this manner shall be secured in order to prevent data breaches (see Parts 29 to 34 of this Policy for details of data security and organisational measures).]

## 23. Personal Data

The Company holds a range of personal data about its employees. Employee personal data shall be collected, stored, processed and used in accordance with employee data subjects' rights and the Company's obligations under Data Protection Law and this Policy. The Company shall not disclose employee personal data and process the employee personal data detailed in Parts 23 to 34 of this Policy. For details of data retention, please refer to the Company's Data Retention Policy.

- 23.1 Identification information (Please refer to Part 24, below, for further information):
- a) Name;
  - b) Contact Details;
  - c) <<add further information>>
- 23.2 Equal opportunities information (Please refer to Part 24, below, for further information):
- a) Age;
  - b) Gender;
  - c) Ethnicity;
  - d) Nationality;
  - e) Religion;
  - f) <<add further information>>
- 23.3 Health records (Please refer to Part 24, below, for further information):
- a) Details of sickness absence;
  - b) Medical conditions;



S

A

M

P

L

E

- c) Disabilities;
- d) Prescribed n
- e) <<add further

#### 23.4 Employment record

- a) Interview no
- b) CVs, applica
- c) Assessment
- d) Details of r
- e) Details of tra
- f) Employee m
- g) Records of
- h) Details of g
- i) <<add further

ers, and similar documents;

and similar documents;

salaries, pay increases, bonuses, expenses;

where applicable) [(please refer to)];

please refer to Part 28, below, for

uding reports and warnings, both

documentary evidence, notes from outcomes;

#### 24. Equal Opportunities Mon

24.1 The Company col  
purposes of moni  
collected for this pu  
falls within the UK  
this Policy for a de  
Where special cate  
processed strictly i  
category personal  
category personal  
collected, held, or  
consent.] OR [The  
<<insert lawful basi  
6.2)>>.]

24.2 [Non-anonymised  
opportunities moni  
<<insert departmen  
employees, agents  
Company [without  
whom such data r  
necessary to prote  
concerned, and suc  
out in Part 6.2 of thi

24.3 Equal opportunities  
processed to the  
discrimination in l  
recruitment, promo  
terms and conditi

sses certain information for the  
es. Some of the personal data  
ethnic origin and religious beliefs,  
pecial category data (see Part 2 of  
e, such data will be anonymised.  
ains, it will be collected, held, and  
conditions for processing special  
rt 6.2 of this Policy. [No special  
opportunities monitoring will be  
relevant employee data subject's  
sis for processing such data is  
category data (as listed under Part

monitoring information] OR [Equal  
be accessible and used only by  
and shall not be revealed to other  
parties working on behalf of the  
the employee data subject(s) to  
otional circumstances where it is  
of the employee data subject(s)  
one or more of the conditions set

will only be collected, held, and  
vent, reduce, and stop unlawful  
Act 2010, and to ensure that  
ment, assessment, benefits, pay,  
edundancy, and dismissals are



S

determined on the basis of their qualifications, experience, skills, and productivity.

- 24.4 Employee data subjects have the right to request that the Company does not keep equal opportunity information about them. All requests must be made in writing and must specify the person's name(s) and/or position(s) and contact details>>.

ifications, experience, skills, and productivity. request that the Company does not keep equal opportunity information about them. All requests must be made in writing and must specify the person's name(s) and/or position(s) and contact details>>.

## 25. Health Records

- 25.1 The Company holds employee data subjects which are used to assess the health and welfare of employees and to highlight any issues for further investigation. In particular, the Company places a high priority on maintaining health and safety in the workplace, on promoting good working conditions, and on preventing discrimination on the grounds of disability. In most cases, health data on employees is collected in accordance with the GDPR's definition of special category data (see Part 2 of this Policy). Any and all data relating to employee data subjects will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data set out in Part 6.2 of this Policy. [No special category personal data will be collected, held, or processed without the employee's explicit consent.] OR [The Company's lawful basis for processing special category personal data is <<insert lawful basis for processing special category personal data>>.]

employee data subjects which are used to assess the health and welfare of employees and to highlight any issues for further investigation. In particular, the Company places a high priority on maintaining health and safety in the workplace, on promoting good working conditions, and on preventing discrimination on the grounds of disability. In most cases, health data on employees is collected in accordance with the GDPR's definition of special category data (see Part 2 of this Policy). Any and all data relating to employee data subjects will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data set out in Part 6.2 of this Policy. [No special category personal data will be collected, held, or processed without the employee's explicit consent.] OR [The Company's lawful basis for processing special category personal data is <<insert lawful basis for processing special category personal data>>.]

- 25.2 Health records shall be held only by <<insert department(s) and/or position(s)>> and shall not be disclosed to other employees, agents, contractors, or other third parties without the prior written consent of <<insert department(s) and/or position(s)>> on behalf of the Company [without the consent of the employee data subject(s) to whom such data relates], except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject, and such circumstances are set out in Part 6.2 of this Policy.

ed only by <<insert department(s) and/or position(s)>> and shall not be disclosed to other employees, agents, contractors, or other third parties without the prior written consent of <<insert department(s) and/or position(s)>> on behalf of the Company [without the consent of the employee data subject(s) to whom such data relates], except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject, and such circumstances are set out in Part 6.2 of this Policy.

- 25.3 Health records will be collected, held, and processed to the extent necessary to ensure that employees can perform their work correctly, safely, and without any impediments or discrimination.

d, and processed to the extent necessary to ensure that employees can perform their work correctly, safely, and without any impediments or discrimination.

- 25.4 Employee data subjects have the right to request that the Company does not keep health records about them. All requests must be made in writing and must specify the person's name(s) and/or position(s) and contact details>>.

request that the Company does not keep health records about them. All requests must be made in writing and must specify the person's name(s) and/or position(s) and contact details>>.

## 26. Benefits

- 26.1 In cases where employees are enrolled in benefit schemes which are provided by the Company or by third party organisations, the Company will ensure that the necessary information is collected from relevant employee data subjects.

enrolled in benefit schemes which are provided by the Company or by third party organisations, the Company will ensure that the necessary information is collected from relevant employee data subjects.

- 26.2 Prior to the collection of any personal data, employee data subjects will be fully informed of the purpose for which the data is being collected, the reasons for its collection, and the requirements set out in Part 6.2 of this Policy.

employee data subjects will be fully informed of the purpose for which the data is being collected, the reasons for its collection, and the requirements set out in Part 6.2 of this Policy.

- 26.3 The Company shall not collect, hold, or process any special category personal data except insofar as is necessary in the administration of benefit schemes.

personal data except insofar as is necessary in the administration of benefit schemes.

- 26.4 The following scheme of benefits shall apply to all employees. Please note that not all

employees. Please note that not all

A

M

P

L

E



schemes may be applied:

- a) <<Insert name of scheme>>. For further information, please contact the relevant trade union(s), position(s), and/or third-party organisation(s) to which the personal data may be collected, held, and processed and its purpose>>;
  - i) <<insert details of scheme>>;
  - ii) <<add further details>>.
- b) [<<Add further details>>.]

## 27. [Trade Unions]

- 27.1 The Company will collect, hold, and process personal data concerning relevant employee data subjects who are members of trade unions where those unions are recognised by the Company. Information about an individual's trade union membership, therefore, will be collected, held, and processed in accordance with the conditions for special category data (see Part 6.2 of this Policy) as set out in Part 6.2 of this Policy. [No special category data relating to trade union membership, therefore, will be collected, held, or processed without the relevant employee data subject's express consent.] **OR** [The Company's lawful basis for processing special category data relating to trade union membership is <<insert lawful basis under Part 6.2>>.]

- a) Name;
- b) Job description;
- c) <<insert type of data>> and its purpose>>;
- d) <<add further details>>.

- 27.2 All employee data subjects have the right to request that the Company does not supply their personal data and shall be informed of that right before any such request is made.

## 28. Employee Monitoring

- 28.1 The Company may monitor the activities of employee data subjects. Such monitoring will not necessarily be limited to internet and email activity, but may include any kind of monitoring of any kind is to take place (unless the monitoring is for the investigation of criminal activity or other serious circumstances, such as the investigation of criminal activity or other serious circumstances, justify covert monitoring), employee data subjects shall be informed of the exact nature of the monitoring in advance.
- 28.2 Monitoring should not be used in a way that interferes with an employee data subject's privacy (unless the circumstances justify it, as above)
- 28.3 Monitoring will only be used where the Company considers that it is necessary to achieve the benefit of the monitoring. Personal data collected during any such monitoring will be held, and processed for reasons directly related to (a) the achievement of the intended result and, at all times, in accordance with the Company's obligations under DPA 2018 and the Company's obligations under the GDPR.



S

- 28.4 The Company shall ensure no unnecessary intrusion upon employee data subject's communications or activities, and under no circumstances will the Company access employee data outside of an employee data subject's normal place of work hours, unless the employee data subject in question consents in writing. This includes, but not limited to, Company email, Company intranet, or a virtual private network ("VPN") server.

A

29. **Data Security - Transfer of Data and Communications**

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

- 29.1 All emails containing employee personal data must be encrypted [using <<insert type(s) of encryption>>];
- 29.2 All emails containing employee personal data must be marked "confidential";
- 29.3 Employee personal data shall be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- 29.4 Employee personal data shall not be transmitted over a wireless network if a secure alternative is reasonably practicable;
- 29.5 Employee personal data, whether sent or received, should be encrypted. The body of an email, whether sent or received, should be encrypted. The header of that email and stored securely. Temporary files associated therewith should be deleted [using <<insert method of deletion>>];
- 29.6 Where employee personal data is transmitted by facsimile transmission the recipient should be notified of the transmission and should be deleted after use;
- 29.7 Where employee personal data is transferred in hardcopy form it should be passed directly to the recipient using <<insert name(s) and/or address>>.
- 29.8 All employee personal data, whether in hardcopy form or on removable storage, shall be transferred in a suitable container marked "Confidential".
- 29.9 [Use <<Add further security measures>>.]

M

P

30. **Data Security - Storage**

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

- 30.1 All electronic copies of employee personal data should be stored securely using passwords and encryption [using <<insert type of encryption>>];
- 30.2 All hardcopies of employee personal data, along with any electronic copies, should be stored securely in a locked container.
- 30.3 All employee personal data should be backed up <<insert frequency>> with backups stored <<insert location>> [on/Off/ON/OR [offsite]]. All backups should be encrypted [using <<insert type of encryption>>];
- 30.4 No employee personal data should be stored on any mobile device (including, but not limited to, smartphones, tablets, or other mobile devices), whether such device is owned by the Company or the employee.

L

E



# SAMPLE

belongs to the Company <<insert name(s) and contact details>> and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time of approval, and for no longer than is absolutely necessary.

without the formal written approval of <<insert name(s) and contact details>> and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time of approval, and for no longer than is absolutely necessary.

30.5 No employee personal data belonging to an employee, agent, contractor, or other party working on behalf of the Company and stored on devices belonging to the Company where the letter and spirit of the law is limited to the UK GDPR, that all suitable technical

transferred to any device personally owned by an employee, agent, contractor, or other party working on behalf of the Company may only be transferred to other parties working on behalf of the Company as agreed to comply fully with the Data Protection Law, including but not limited to demonstrating to the Company that appropriate measures have been taken);

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

>>].

## 31. Data Security - Disposal

When any employee personal data or otherwise disposed of for any reason (including where copies are no longer needed), it should be securely deleted and the Company should maintain information on the deletion and disposal of personal data, per its Data Retention Policy.

When any employee personal data or otherwise disposed of for any reason (including where copies are no longer needed), it should be securely deleted and the Company should maintain information on the deletion and disposal of personal data, per its Data Retention Policy.

## 32. Data Security - Use of Personal Data

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

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

32.1 No employee personal data shall be accessed informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any employee personal data, they do not already have access to, such access shall be requested from <<insert name(s) and/or position(s) and contact details>>.

32.1 No employee personal data shall be accessed informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any employee personal data, they do not already have access to, such access shall be requested from <<insert name(s) and/or position(s) and contact details>>.

32.2 No employee personal data shall be transferred to any employee, agent, contractor, or other party working on behalf of the Company or not, without the written approval of <<insert name(s) and/or position(s) and contact details>>.

32.2 No employee personal data shall be transferred to any employee, agent, contractor, or other party working on behalf of the Company or not, without the written approval of <<insert name(s) and/or position(s) and contact details>>.

32.3 Employee personal data shall be handled with care at all times and should not be left unattended or accessible to employees, agents, contractors, or other parties at any time.

32.3 Employee personal data shall be handled with care at all times and should not be left unattended or accessible to employees, agents, contractors, or other parties at any time.

32.4 If employee personal data is displayed on a computer screen and the computer in question is left unattended for any period of time, the user must lock the computer.

32.4 If employee personal data is displayed on a computer screen and the computer in question is left unattended for any period of time, the user must lock the computer.

32.5 [Where employee personal data is used for marketing purposes, it shall be used in accordance with appropriate consent or opt-out, whether or not the employee has opted out, whether or not the employee has opted out, whether or not the employee has opted out.]

32.5 [Where employee personal data is used for marketing purposes, it shall be used in accordance with appropriate consent or opt-out, whether or not the employee has opted out, whether or not the employee has opted out, whether or not the employee has opted out.]

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

>>].

## 33. Data Security - IT Security

The Company shall ensure appropriate measures are taken with respect to IT

The Company shall ensure appropriate measures are taken with respect to IT



and information security:

- 33.1 All passwords used for accessing personal data should be changed regularly and should not be easily guessed or otherwise compromised. Passwords must contain a combination of uppercase and lowercase letters, numbers and symbols. [All software used by the Company is configured to enforce these password requirements.];
- 33.2 Under no circumstances should passwords be written down or shared between any employees, contractors, or other parties working on behalf of the Company. Passwords should be stored securely, by priority or department. If a password is forgotten, it must be reset using a secure method. IT staff do not have access to passwords.
- 33.3 All software (including applications and operating systems) shall be kept up-to-date. IT staff shall be responsible for installing any and all updates [not more than <<insert period>> after the release date of the manufacturer] OR [if updates are available by the publisher or manufacturer and practically possible] [, unless there are valid technical reasons not to do so];
- 33.4 No software may be installed on a company-owned computer or device without the prior approval of the IT department or position>>;
- 33.5 [ <<Add further security measures as appropriate>>.]

#### 34. Organisational Measures

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

- 34.1 All employees, agents, contractors, or 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;
- 34.2 Only employees, agents, contractors, or parties working on behalf of the Company that need to process employee personal data in order to carry out their assigned duties shall have access to employee personal data held by the Company;
- 34.3 All sharing of employee personal data shall comply with the information provided to the relevant subjects and, if required, the consent of such data subjects or to the sharing of their personal data;
- 34.4 All employees, agents, contractors, or parties working on behalf of the Company handling employee personal data will be appropriately trained to do so;
- 34.5 All employees, agents, contractors, or parties working on behalf of the Company handling employee personal data will be appropriately supervised;
- 34.6 All employees, agents, contractors, or parties working on behalf of the Company handling employee personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters in the workplace or otherwise;
- 34.7 Methods of collecting, holding, and processing employee personal data shall be regularly evaluated and updated as appropriate.



# SAMPLE

- 34.8 All employee personal data shall be reviewed periodically, as set out in the Company's Data Retention Policy;
- 34.9 The performance of agents, contractors, or other parties working on behalf of the Company in relation to employee personal data shall be regularly evaluated;
- 34.10 All employees, agents, contractors, or other parties working on behalf of the Company handling employee personal data will be bound to do so in accordance with the Data Protection Law and this Policy by contract;
- 34.11 All agents, contractors, or other parties working on behalf of the Company handling employee personal data shall ensure that any and all of their processing of employee personal data are compliant with the Data Protection Law; relevant employees of the Company shall also be bound by the Data Protection Law;
- 34.12 Where any agent, contractor, or other party working on behalf of the Company handling employee personal data, that party shall indemnify the Company against any costs, damages, or liabilities which may arise out of that party's failure to comply with this Policy;
- 34.13 [ <<Add further organisational measures as required>>.]

## 35. Sharing Personal Data

- 35.1 The Company may share employee personal data with third parties if specific safeguards are in place.
- 35.2 Employee personal data may be shared with other employees, agents, contractors, or other parties working on behalf of the Company if the recipient has a legitimate, job-related need for the data. If any employee personal data is to be shared with a third party outside of the UK, the provisions of Part 36, below, shall also apply.
- 35.3 Where a third-party processor is used, that processor shall process employee personal data only on the written instruction of the Company (as data controller) and in accordance with the following conditions:
- 35.4 Employee personal data shall not be shared with third parties in the following circumstances:
- a) the third party is not bound to know the information for the purpose of processing the data on behalf of the Company under a contract;
  - b) the sharing of the data does not comply with the privacy requirements of the Data Protection Law, Part 15 for the processing of employee personal data concerned hereunder; and, if required, the employees concerned have given their consent to the sharing of their personal data;
  - c) the third-party processor is not bound to comply with all applicable data protection procedures, and has put in place measures to protect the employee personal data;
  - d) (where applicable) the sharing of the data does not comply with any cross-border transfer restrictions (if any) applicable to the data.



- e) a fully executed contract containing data processing clauses compliant with the GDPR. A contract has been entered into with the third-party recipient.

## 36. Transferring Personal Data Outside the UK

- 36.1 The Company may transfer personal data available remotely) to countries outside of the UK. The UK GDPR requires the Company to ensure that the level of protection given to data subjects is not compromised.
- 36.2 Employee personal data may be transferred to a country outside the UK if one of the following conditions is met:
- a) The UK has been deemed to ensure an 'adequacy' of decisions' of the European Commission. From 1 January 2021, transfers of personal data to EEA countries will continue to be permitted. The Commission has also in place to recognise pre-existing EU adequacy decisions.
  - b) Appropriate safeguards, including binding corporate rules, are in place for use in the UK (this includes those adopted by the Commission prior to 1 January 2021), or an approved certification mechanism.
  - c) The transfer is necessary for the performance of a contract and explicit consent of the data subject.
  - d) The transfer is necessary for the other reasons set out in the UK GDPR including: to perform a contract between the employee and the Company; for public interest reasons; for the establishment, exercise or defence of legal claims; to protect the vital interests of the data subject where the employee data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

## 37. Data Breach Notification

- 37.1 All personal data breaches must be reported immediately to the Data Protection Officer.
- 37.2 If an employee, agent or third 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 in question should be carefully retained.
- 37.3 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, or other significant damage, or other significant damage), the Data Protection Officer must ensure that the breach is reported to the relevant supervisory authority without delay, and in any event, within 72 hours of becoming aware of it.
- 37.4 In the event that a personal data breach is likely to result in a high risk (that is, a breach likely to result in a high risk to the rights and freedoms of individuals), the Data Protection Officer must ensure that all affected individuals are notified without delay.



S

affected employee  
without undue delay

med of the breach directly and

37.5 Data breach notification

llowing information:

- a) The category
- b) The category  
concerned;
- c) The name and  
(or other contact  
information);
- d) The likely consequences;
- e) Details of the  
Company's  
measures to

ber of data subjects concerned;  
number of personal data records  
Company's data protection officer  
information can be obtained);  
ch;  
proposed to be taken, by the  
including, where appropriate,  
verse effects.

38. Implementation of Policy

This Policy shall be deemed  
shall have retroactive effect  
this date.

ert date>>. No part of this Policy  
only to matters occurring on or after

This Policy has been approved and

**Name:** <<insert>>

**Position:** <<insert>>

**Date:** <<insert>>

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

**Signature:**

A

M

P

L

E