

S

A

M

P

L

E

1. Introduction

This Policy sets out the registered in <<insert company registration number>>, with the Company) regarding data "employee data subjects" under the Data Protection Legislation (defined below)

This Policy sets out the Company's policy regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. 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.

Company name>>, a company registered under number <<insert company registration number>>, with its office located at <<insert address>> ("the Company") regarding data subjects of its employees (in this context, "employee data subjects") under the Data Protection Legislation (defined below)

This Policy sets out the Company's policy regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. 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"

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

"data controller"

any natural or legal person or organisation 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 processor"

any person or organisation which processes personal data on behalf of a data controller;

"Data Protection Legislation"

the applicable data protection and privacy legislation, including, but not limited to, the Data Protection Act 1998, any applicable national laws, regulations, and secondary legislation in the United Kingdom and Wales concerning the processing of personal data or the privacy of electronic communications, as amended, replaced, or otherwise in force from time to time;

"data subject"

any living, identified, or identifiable individual about whom the Company holds personal data (in this context, employee data subjects)

S

“EEA”

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

“personal data”

A

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

“personal data breach”

M

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

“processing”

any operation or set of operations which are 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 restriction, erasure or destruction;

“pseudonymisation”

P

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 linked to an identified or identifiable natural person; and

“special category personal data”

L

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

3. Data Protection Officer &

3.1 The Company’s Data Protection Officer is <<insert name of data protection officer>>, <<insert name of Data Protection Officer responsible [ , work email address] >>

<<insert name of data protection officer>>, <<insert name of the Data Protection Officer responsible [ , work email address] >> <<insert department, e.g. HR >>

E



S

- 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.

A

**6. Lawful, Fair, and Transparent**

6.1 The Data Protection Act 2018 requires that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful only if one of the following applies:

- a) the data subject has given their 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 in order 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.

M

6.2 If the personal data is of a special category (also known as ‘sensitive personal data’) then the following conditions must be met in addition to one of the conditions set out above:

- a) the data subject has given their explicit consent to the processing of their special category personal data for one or more specific purposes (unless EU or EU Member State law prohibits the controller 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 social security, social insurance, social security, and social protection law or a collective agreement, provided that the law or a collective agreement provides for appropriate safeguards for the fundamental rights and freedoms of the data subject; or
- c) the processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is unable to give consent;

P

L

E

S

d) the data controller with a political or trade union aim, and the processing of the data is necessary for the course of its legitimate activities, provided that the data is not disclosed or made available solely to the members or former members of the association, or other non-profit body who have regular contact with it in connection with its activities, and that the personal data is not processed for the purpose of the consent of the data subjects;

A

e) the processing of the data which is manifestly made public by the data controller;

M

f) the processing of the data for the conduct of legal claims or for the exercise of the judicial capacity;

P

g) the processing of the data on substantial public interest reasons, on the basis of the law which shall be proportionate to the aim pursued, and of the essence of the right to data protection, and which provides for suitable and specific measures to safeguard the fundamental interests of the data subject;

L

h) the processing of the data for occupational health purposes, for the assessment of the working capacity of an employee, for the diagnosis, care or treatment of an employee or for the provision of health or social care or treatment or services of a contract worker, subject to the conditions and safeguards laid down in the law of the Member State law or pursuant to national law or pursuant to collective agreements, subject to the conditions and safeguards laid down in the law of the Member State;

E

i) the processing of the data for public interest reasons in the area of public health, for the prevention of serious cross-border threats to health, for the management of health care systems or medical devices, on the basis of the law of the Member State which provides for suitable and specific measures to safeguard the fundamental freedoms of the data subject (in particular, the right to the protection of personal data);

j) the processing of the data for archiving purposes in the public interest, scientific or statistical purposes, or for statistical purposes in the area of social science, on the basis of the law of the Member State, which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

**7. Consent**

If consent is relied upon as the legal basis for the collection, storing, holding, and/or processing of any personal data, the following conditions apply:

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

7.2 Where consent is obtained as part of a contract or other legal agreement which includes other matters, the consent to the processing of personal data 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

S

easy for them to do  
be honoured promptly

draws consent, their request must

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

erent purpose that is incompatible with the original purpose for which that personal data was originally collected from a subject when they first provided their consent. The original purpose or purposes may need to be identified

7.5 Where special category data is processed, the Company shall normally rely on a legal basis other than implicit consent. If explicit consent is used, it must be issued with a suitable privacy notice in order to ensure that the data subject is aware of what is being done with their data

processed, the Company shall obtain explicit consent. If explicit consent is used, it must be issued with a suitable privacy notice in order to ensure that the data subject is aware of what is being done with their data

7.6 In all cases where the Company processes personal data on the basis of consent, records must be kept of all consents obtained in order to demonstrate compliance with consent requirements

as the lawful basis for collecting, using, disclosing and otherwise processing records must be kept of all consents obtained in order to demonstrate compliance with consent requirements

**8. Specified, Explicit, and Limited**

M

8.1 The Company collects and processes employee personal data set out in Part 23 of this Policy

employee personal data set out in Part 23 of this Policy

a) personal data of employee data subjects and]

employee data subjects[.] OR [;

b) [personal data of employee data subjects.]

ties.]

8.2 The Company only holds employee personal data for the specific purposes expressly permitted by this Policy (or for other purposes permitted by legislation).

holds employee personal data for the specific purposes expressly permitted by this Policy (or for other purposes permitted by legislation).

8.3 Employee data subjects must be informed at all times of the purpose or purposes for which their personal data is collected. Please refer to Part 15 for more information.

must be informed at all times of the purpose or purposes for which their personal data is collected. Please refer to Part 15 for more information.

**9. Adequate, Relevant, and**

P

9.1 The Company will collect and process 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 23 of this Policy

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 23 of this Policy

9.2 Employees, agents and other parties working on behalf of the Company may collect and process personal data only to the extent required for the performance of their job duties. Excessive personal data must not be collected.

Employees, agents and other parties working on behalf of the Company may collect and process personal data only to the extent required for the performance of their job duties. Excessive personal data must not be collected.

9.3 Employees, agents and other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for other purposes.

Employees, agents and other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for other purposes.

**10. Accuracy of Data and Keeping**

L

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, ensuring that

employee personal data collected, processed, and held is accurate and up-to-date. This includes, but is not limited to, ensuring that

E

S

A

M

P

L

E

not limited to, the re  
data subject, as set

ata at the request of an employee

10.2 The accuracy of em  
and at [regular] OR  
personal data is fou  
be taken without de

all be checked when it is collected  
ervals thereafter. If any employee  
ut-of-date, all reasonable steps will  
at data, as appropriate.

10.3 It is the responsibil  
personal data they  
such personal data  
member of staff a  
possible. The Com  
meet its obligations

the data subjects to ensure that the  
ompany is kept up-to-date. If any  
should ensure that the relevant  
ormed as soon as is reasonably  
operation of its employees to help  
n Legislation.

**11. Data Retention**

11.1 The Company shall  
necessary in light  
collected, held, and

personal data for any longer than is  
poses for which it was originally

11.2 When employee pe  
be taken to erase o

required, all reasonable steps will  
securely and without delay.

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

**12. Secure Processing**

12.1 The Company shall  
and processed is k  
processing and ag  
details of the techn  
provided in the C  
Policy].

ee personal data collected, held,  
d against unauthorised or unlawful  
destruction, or damage. Further  
measures which shall be taken are  
ty Policy] AND/OR [IT Security

12.2 All technical and or  
data shall be reg  
effectiveness and th

taken to protect employee personal  
evaluated to ensure their ongoing  
employee personal data.

12.3 Data security must  
integrity, and availa

es by protecting the confidentiality,  
sonal data as follows:

- a) only those w  
data and wh
- b) employee pe  
or purposes
- c) authorised u  
data as requ

- ccess and use employee personal  
y may access and use it;
- urate and suitable for the purpose  
held, and processed; and
- ple to access employee personal  
purpose or purposes.

**13. Accountability and Record**

13.1 The Data Protection  
<<insert departmen  
for administering t

nsible [, working together with the  
or position, e.g. HR Manager>>],  
veloping and implementing any

S

A

M

P

L

E

applicable related policies and procedures or guidelines.

13.2 The Company shall ensure that its 'Privacy by Design' approach at all times when collecting, holding, processing, or otherwise using personal data. Data Protection Impact Assessments shall be conducted where 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 applicable data protection legislation, this Policy, and all other applicable policies and procedures.

13.4 The Company's data protection policies shall be regularly reviewed and updated as necessary.

13.5 The Company shall ensure that its records of all employee personal data collection, holding, processing, and use shall incorporate the following:

- a) the name and contact details of the Company, its Data Protection Officer, and any applicable data protection officers (including data processors and other data controllers);
- b) the purpose of the data collection, how the Company collects, holds, and processes the data;
- c) the Company's legal basis for processing (including, where applicable, employee consent, the Company's consent policy, and records of such consent);
- d) details of the data collection, including the categories of employee 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 data transfers of employee personal data to non-EEA countries including the legal basis and security safeguards;
- f) details of how long the employee personal data will be retained by the Company (please refer to the Company's Data Retention Policy);
- g) details of employee personal data storage, including location(s); and
- 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 (DPIA) and Privacy by Design**

14.1 In accordance with the Company's Data Protection Impact Assessment (DPIA) Policy, the Company shall carry out DPIAs for all new projects and/or new uses of employee personal data that involve the use of new technologies and where the processing is likely to result in a high risk to the rights and freedoms of employee data subjects.

14.2 The principles of 'Privacy by Design' shall be followed at all times when collecting, holding, processing, or otherwise using personal data. The following factors should be taken into account when conducting a DPIA:

- a) the nature, scope, and context of the processing, the purpose or purposes of the collection,



S

- b) the state of the art technical and organisational measures to
- c) the cost of implementation; and
- d) the risks posed to the data subjects and to the Company, including the

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

- 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 legitimate interests in the use of the data;
- d) how employee personal data will be used;
- e) the parties (if any) to whom the data is to be shared; and 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 data subjects; and
- h) risks posed to the Company; and
- i) proposed measures to mitigate the risks.

A

M

15. Keeping Data Subjects Informed

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

- a) Where employee 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 data is obtained from a third party, the relevant employee data subject will be informed of its purpose:
  - i) if the data subject is to be contacted to communicate with the employee; 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.

P

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

- a) details of the data controller, including contact details, and details of any applicable representative; and
- b) the purpose(s) for which the personal data is being collected and will be processed (as set out in Part 23 of this Policy) and the lawful basis for the collection and processing;
- c) where applicable, the legal basis upon which the Company is relying for the collection and processing of the employee personal data;

L

E

S

d) where the employee data is not obtained directly from the employee data subject; details of personal data collected and processed;

e) where the employee data is to be transferred to one or more third parties;

f) where the employee 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 destination country (see Part 25 of this Policy for further details);

g) details of applicable retention periods;

h) details of the employee data subject's rights under the Data Protection Legislation;

i) details of the employee data subject's right to withdraw their consent to the Company's processing of their personal data at any time (where applicable);

j) details of the employee data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority');

k) where the employee data is not obtained directly from the employee data subject, the source of that personal data;

l) where applicable, the legal or contractual requirement or obligation necessitating the collection and processing of the employee data, and the consequences of failing to provide it;

m) details of any automated decision-making or profiling that will take place using the employee data, including information on how those decisions will be made, the consequences of those decisions, and any other relevant information.

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 personal data which the Company holds about them, what it is doing with that data, and why.

16.2 Employees wishing to exercise their right to access should do so using a Subject Access Request Form, sent to the Company's Data Protection Officer at <<insert contact details>>.

16.3 Responses to SARs will be made within one month of receipt; however, this may be extended to two months if the SAR is complex and/or numerous requests are received. In such additional time is required, the employee data subject shall be notified.

16.4 All SARs received should be handled by the Company's Data Protection Officer in accordance with the 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 already been provided to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repeated.

A

M

P

L

E



S

the amount of employees that is necessary to process the data further.

concerning that data subject (if any) and the data in question is not processed

19.2 In the event that any personal data has been disclosed to third parties, those parties shall be notified of the applicable restrictions on their processing it (unless doing so would require disproportionate effort to do so).

personal data has been disclosed to third parties, those parties shall be notified of the applicable restrictions on their processing it (unless doing so would require disproportionate effort to do so).

20. **[Data Portability**

A

20.1 The Company processes personal data relating to employees using automated means.

personal data relating to employees using automated processing>>.

20.2 Where employee data is processed for purposes other than those for which their consent to the Company to process their personal data was obtained, the Company shall obtain their consent in a manner, or the processing is necessary for the performance of a contract between the Company and the employee data subject, the employee data subjects have the right, under the Data Protection Legislation, to obtain a copy of their personal data and to have it transferred to another data controller (subject to certain conditions).

Where employee data is processed for purposes other than those for which their consent to the Company to process their personal data was obtained, the Company shall obtain their consent in a manner, or the processing is necessary for the performance of a contract between the Company and the employee data subject, the employee data subjects have the right, under the Data Protection Legislation, to obtain a copy of their personal data and to have it transferred to another data controller (subject to certain conditions).

20.3 To facilitate the right of access to applicable personal data, the Company shall make available all personal data in the following format[s]:

To facilitate the right of access to applicable personal data, the Company shall make available all personal data in the following format[s]:

- a) <<list format>>
- b) <<add further details>>

20.4 Where technically feasible, the Company shall provide personal data to the employee data subject in a structured, commonly used and machine-readable format.

Where technically feasible, the Company shall provide personal data to the employee data subject in a structured, commonly used and machine-readable format.

20.5 All requests for access to personal data shall be complied with within one month of receipt of the request. The period can be extended by up to two months in the case of complex or numerous requests. If the Company extends the period, the employee data subject shall be informed.]

All requests for access to personal data shall be complied with within one month of receipt of the request. The period can be extended by up to two months in the case of complex or numerous requests. If the Company extends the period, the employee data subject shall be informed.]

21. **Objections to Personal Data Processing**

M

21.1 Employee data subjects have the right to object to the Company processing their personal data for direct marketing purposes, for scientific and/or historical research and statistics purposes.

Employee data subjects have the right to object to the Company processing their personal data for direct marketing purposes, for scientific and/or historical research and statistics purposes.

21.2 Where an employee data subject objects to the Company processing their personal data based on legitimate grounds, the Company shall cease such processing immediately unless the Company can demonstrate that the Company's legitimate interests, rights, and freedoms override the employee data subject's interests, rights, and freedoms. Where such processing is necessary for the conduct of legal claims, the Company shall continue to process the data.

Where an employee data subject objects to the Company processing their personal data based on legitimate grounds, the Company shall cease such processing immediately unless the Company can demonstrate that the Company's legitimate interests, rights, and freedoms override the employee data subject's interests, rights, and freedoms. Where such processing is necessary for the conduct of legal claims, the Company shall continue to process the data.

21.3 Where an employee data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

Where an employee data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

21.4 Where an employee data subject objects to the Company processing their personal data for scientific and statistics purposes, the Company shall cease such processing unless the employee data subject can demonstrate grounds for the processing. Where such processing is necessary for the performance of a contract, the Company shall continue to process the data.

Where an employee data subject objects to the Company processing their personal data for scientific and statistics purposes, the Company shall cease such processing unless the employee data subject can demonstrate grounds for the processing. Where such processing is necessary for the performance of a contract, the Company shall continue to process the data.

P

L

E

S

A

M

P

L

E

task carried out for

22. **[Automated Processing, Decision-Making, and Profiling**

22.1 [The Company uses automated decision-making processes involving its employees in automated

a) <<Insert out

22.2 [The Company uses automated decision-making processes involving its employees for profiling purposes as follows

a) <<Insert out

22.3 The activities outlined in <<insert location(s)>> are carried out where the resulting data has a similarly significant effect on data subjects unless one of the following applies:

a) the data subject has given explicit consent;

b) the processing is necessary for

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 carried out 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 through automated processing (including profiling), employee data subjects must be given the right to object, to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation from the Company. Employee data subjects must be explained at the first point of contact.

22.6 In addition to the above, employee data subjects must be provided with information explaining the decision-making or profiling, and the significance and consequences of the decision or decisions.

22.7 When employee personal data is processed in any form of automated processing, the following shall apply:

a) appropriate technical and organisational procedures shall be used;

b) technical and organisational measures shall be implemented to minimise the risk of a breach occurring, such measures must enable them to be effectively managed;

c) all personal data processed in this manner shall be secured in order to prevent unauthorised access arising.]

23. **Personal Data**

The Company collects, holds and processes personal data about its employees at all times in accordance with its obligations under the Data Protection Act 2018 and this Policy.

For details of data retention periods, please refer to the Company's Data Retention Policy.

S

A

M

P

L

E

**Special Category Personal Data**

- 23.1 Any and all special category personal data collected, held, and processed will be used in accordance with the applicable conditions set out in Part 6 of this Policy.
- 23.2 Special category personal data will only be collected, held, and processed where it is necessary to protect the interests of the Company, and such data shall be processed and shall not be disclosed to other employees, contractors, or other parties working on behalf of the Company, except in exceptional circumstances where it is necessary to protect the interests of the employee data subject(s) concerned, and such data shall be processed in accordance with the applicable conditions set out in Part 6 of this Policy.

personal data collected, held, and processed will be used in accordance with the applicable conditions set out in Part 6 of this Policy.

Special category personal data will only be collected, held, and processed where it is necessary to protect the interests of the Company, and such data shall be processed and shall not be disclosed to other employees, contractors, or other parties working on behalf of the Company, except in exceptional circumstances where it is necessary to protect the interests of the employee data subject(s) concerned, and such data shall be processed in accordance with the applicable conditions set out in Part 6 of this Policy.

**Identification Information**

- 23.3 The following identification information will be collected, held, and processed:
  - a) Name;
  - b) Contact Details;
  - c) <<add further information>>

will be collected, held, and processed:

**Employment Records**

- 23.4 The following information will be collected, held, and processed:
  - a) Interview notes;
  - b) CVs, applications, and similar documents;
  - c) Assessment reports and similar documents;
  - d) Details of remuneration, including salaries, pay increases, bonuses, expenses;
  - e) Records of disciplinary proceedings, including reports and warnings, both formal and informal;
  - f) Details of grievance procedures, including interviews, reports, and outcomes;
  - g) <<add further information>>

will be collected, held, and processed:

- a) Interview notes;
- b) CVs, applications, and similar documents;
- c) Assessment reports and similar documents;
- d) Details of remuneration, including salaries, pay increases, bonuses, expenses;
- e) Records of disciplinary proceedings, including reports and warnings, both formal and informal;
- f) Details of grievance procedures, including interviews, reports, and outcomes;
- g) <<add further information>>

**Equal Opportunities Monitoring**

- 23.5 Equal opportunities monitoring data will be collected, held, and processed. Where possible, such data shall be anonymised. The Company will use special category personal data for equal opportunities monitoring [only where necessary] [on the lawful basis of <<insert applicable legal basis>>].
- 23.6 Such data will only be collected, held, and processed where it is required to reduce, stop, and prevent unlawful discrimination in recruitment, promotion, training, development, assessment, and dismissals are based on the basis of capability, qualifications, experience, skills, and other objective criteria.
- 23.7 Employees may request that the Company does not hold such data about them. All requests must be made in writing and addressed to <<insert name(s) and position(s)>>.
- 23.8 The following information will be collected, held, and processed:

Equal opportunities monitoring data will be collected, held, and processed. Where possible, such data shall be anonymised. The Company will use special category personal data for equal opportunities monitoring [only where necessary] [on the lawful basis of <<insert applicable legal basis>>].

Such data will only be collected, held, and processed where it is required to reduce, stop, and prevent unlawful discrimination in recruitment, promotion, training, development, assessment, and dismissals are based on the basis of capability, qualifications, experience, skills, and other objective criteria.

Employees may request that the Company does not hold such data about them. All requests must be made in writing and addressed to <<insert name(s) and position(s)>>.

The following information will be collected, held, and processed:

- a) Age;
- b) Gender;
- c) Ethnicity;
- d) Nationality;
- e) Religion;
- f) <<add further

**Health Records**

- 23.9 Health information constitutes special category personal data. The Company will use special category employee data subject information for the lawful basis (as listed in Part 6)
- 23.10 Health data will be processed to the extent required to ensure that employees are able to work safely, correctly, legally, safely, and without discrimination.
- 23.11 Employees may request that the Company does not hold such data about them. All requests must be made in writing and addressed to <<insert name(s) and position(s)>>.
- 23.12 The following information will be held, and processed:
  - a) Details of sickness absence;
  - b) Medical conditions;
  - c) Disabilities;
  - d) Prescribed medication;
  - e) <<add further

**Benefits**

- 23.13 If an employee is eligible for a benefit offered by the Company, it may be necessary for the Company to collect personal data from the employee. Any special category data provided with the necessary information prior to the collection of their data (as per the information requirements set out in Part 6).
- 23.14 The Company shall not disclose personal data except to the extent necessary for the administration of relevant benefits schemes.

**[Trade Union Data**

- 23.15 The Company will process special category data about relevant employees to support the administration of relevant benefits (Company). Most data about an employee's trade union membership constitutes special category personal data. The Company will process such data for the purposes [only with employee data subject's consent] (as per the information requirements of <<insert lawful basis (as listed in Part 6)>>)].
- 23.16 Employees may request that the Company does not supply their personal data to trade unions and other third parties. All requests must be made in writing right before any transfer is made.
- 23.17 The following information will be held, and processed:
  - a) Name;

S

A

M

P

L

E

- b) Job description
- c) <<insert type>> purpose>>;
- d) <<add further>>

**Employee Monitoring**

- 23.18 The Company may monitor employees' activities, such as internet and email usage, for exceptional circumstances (such as criminal investigations or disciplinary proceedings of a severity) justify covert monitoring, and employees will be informed of such monitoring in advance. Monitoring shall not normally interfere with an employee's duties.
- 23.19 Monitoring will take place where the Company considers it necessary. Personal data collected for such purposes will only be collected, held, used, and necessary for, achieving the intended result. Monitoring shall be conducted in accordance with applicable Legislation.
- 23.20 Intrusion upon employees' communications and activities will be avoided whenever possible. In exceptional circumstances will monitoring take place outside of an employee's normal place of work or working hours unless the employee is using Company facilities such as Company email, internet access, or other facilities provided by the Company for its employees.

**24. Sharing Personal Data**

- 24.1 The Company may share employee personal data with third parties if specific safeguards are in place.
- 24.2 Employee personal data may be shared with other employees, agents, contractors, or other representatives of the Company if the recipient has a legitimate, job-related purpose and any employee personal data is to be shared with a third party outside of the European Economic Area, the provisions of Part 15 shall apply.
- 24.3 Where a third-party processor is used, that processor shall process personal data on behalf of the Company (as data controller) only on the written instruction of the Company.
- 24.4 Employee personal data may be shared with third parties in the following circumstances:
  - a) the third party is required to know the information for the purpose of providing services to the Company under a contract;
  - b) the sharing of the personal data concerned complies with the privacy requirements of the Company and the affected employee data subjects (see Part 15 for more details) have consented, and, if required, the employees have agreed to the sharing of their personal data;
  - c) the third-party processor is required to comply with all applicable data protection laws, procedures, and has put in place adequate security measures to protect the employee personal data;
  - d) (where applicable) the sharing complies with any cross-border transfer restrictions (see Part 15 for more details);
  - e) the sharing is done through a fully executed data processing agreement containing GDPR-approved third-party clauses and is done in accordance with the third-party recipient.



S

25. **Transferring Personal Data to the [UK and] EEA**

25.1 The Company may make personal data available remotely) to countries outside of the [UK and] EEA.

25.2 The transfer of employee personal data to a country outside of the [UK and] EEA shall take place in one or more of the following ways:

- a) the transfer of personal data to a country outside of the [UK and] EEA where the recipient is a public authority or one or more specific sectors in that country (including a public authority or organisation), that the European Commission has determined provides an adequate level of protection for personal data;
- b) the transfer of personal data to a country outside of the [UK and] EEA where the recipient is an international organisation (including a public authority or organisation) which provides appropriate safeguards in the form of a legally binding agreement or arrangement with an approved controller or bodies; binding corporate rules; standard contractual clauses adopted by the European Commission; approved codes of conduct approved by a supervisory authority; certification or accreditation by a supervisory authority; certification for in the Data Protection Act 2018; or contractual clauses authorised by a supervisory authority; or provisions inserted into contracts between public authorities or bodies authorised by a supervisory authority;
- c) the transfer of personal data to a country outside of the [UK and] EEA with the informed and explicit consent of the relevant employee;
- d) the transfer of personal data to a country outside of the [UK and] EEA for the performance of a contract between the employee and the Company (or for pre-contractual steps taken at the request of the employee data subject);
- e) the transfer of personal data to a country outside of the [UK and] EEA for public interest reasons;
- f) the transfer of personal data to a country outside of the [UK and] EEA in connection with the pursuit of legal claims;
- g) the transfer of personal data to a country outside of the [UK and] EEA where the vital interests of the employee data subject require it and where the employee data subject is unable to give their consent; or
- h) the transfer of personal data to a country outside of the [UK and] EEA where that, under UK or EU law, is necessary for the performance of a task in the public interest and which is open for public access by the public and which is otherwise to those who are able to access the register.

A

M

P

L

E

26. **Data Breach Notification**

26.1 All personal data breaches involving employee personal data must be reported immediately to the Data Protection Officer.

26.2 If an employee, agent or contractor of the Company becomes aware that a personal data breach has occurred, they must report it immediately. Any and all evidence relating to the breach should be carefully retained.

26.3 If a personal data breach is likely to result in a risk to the rights and freedoms of natural persons (e.g. financial loss, breach

S

of confidentiality, of social or economic Information Commi and in any event, w

nal damage, or other significant ection Officer must ensure that the ned of the breach without delay, g become aware of it.

26.4 In the event that a p a higher risk than th employee data sub affected employee without undue delay

likely to result in a high risk (that is, 26.3) to the rights and freedoms of tion Officer must ensure that all rmed of the breach directly and

26.5 Data breach notifica

llowing information:

- a) The categor
- b) The categor concerned;
- c) The name a (or other cor
- d) The likely co
- e) Details of t Company t measures to

- ber of data subjects concerned;
- umber of personal data records
- Company's data protection officer formation can be obtained);
- h;
- r proposed to be taken, by the n including, where appropriate, erse effects.

27. **Implementation of Policy**

This Policy shall be deem shall have retroactive effec this date.

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

This Policy has been approved an

**Name:** <<insert

**Position:** <<insert

**Date:** <<insert

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

**Signature:**

A

M

P

L

E