Data Protection Policy (for Employees, Workers, Consultants and Job Applicants)

1. Introduction

1.1. The Overview

1.1.1. This Policy sets out the obligations of Colorminium London Ltd., a Company registered in England & Wales under number 01799913, whose registered office is at Saxon House, 23 Springfield Lyons Approach, Chelmsford, Essex, CM2 5LB ("the Company") regarding data protection, privacy and the rights of its employees.

1.1.2. The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this Policy.

1.1.3. The GDPR defines "*personal data*" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.1.4. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.1.5. This Policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a '*data subject'* for the purposes of this Policy. You should read this Policy alongside your Contract of Employment (or Contract for Services) and any other notice we issue to you from time to time in relation to your data.

1.1.6. This Policy does not form part of your Contract of Employment (or Contract for Services, if relevant) and can be amended by the Company at any time. It is intended that this Policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this

Policy, the Company intends to comply with the 2018 Act and the GDPR.

1.2. Company Obligations

1.2.1. This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

1.2.2. The Company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from the Human Resources Department.

1.2.3. The Company has measures in place to protect the security of your data in accordance with our IT and Communications Policy and Data Retention Policy. Copies of these can be found on Breathe HR.

1.2.4. The Company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from the Human Resources Department. We will only hold data for as long as necessary for the purposes for which we collected it.

2. Data Protection Principles

2.1. This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following six principles with which any party handling personal data must comply. All personal data must be:

2.1.1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.1.2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.1.3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.1.4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.1.5. Kept in a form which permits 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 for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.1.6. 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.

3. How we define personal data

3.1.'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2.This Policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.2.1. On our website, we use cookies. You will need to consent to us storing this data when going onto our website.

3.3.This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the Contract of Employment (or Services) or after its termination. It could be created by your manager or other colleagues.

3.4.We may collect and use any of the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;

- information about your Contract of Employment (or Services) including start and end dates of employment, role and location, working days and hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement (and previous leave taken);
- information about medical or health conditions, including whether or not you have a disability for which the Company needs to make reasonable adjustments;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- details of your qualifications, skills, experience, training records and employment history, including start and end dates, with previous employers and with the Company;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems etc.;
- your images (whether captured on CCTV, by photograph or video);
- and any other category of personal data which we may notify you of from time to time.

4. How we define processing

4.1. 'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

5. How will we process your personal data?

5.1. The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

5.2. We will use your personal data for:

- performing the Contract of Employment (or Services) between us;
- complying with any legal obligation; or

- if it is necessary for our legitimate interests (or for the legitimate interests of someone else).

  However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

5.3. We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

5.4. If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability that you may suffer from.

6. Examples of when we might process your personal data

6.1. We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

6.2. For example (and see section 6.6 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;

- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- and for any other reason which we may notify you of from time to time.

6.3. We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Human Resources Department.

6.4. We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

6.5. We might process special categories of your personal data for the purposes in paragraph 6.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

6.6. The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which employee data subjects have been informed (or will be informed), as set out in this section 6.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of an employee data subject, as set out in Section 11,
("Rectification") below.

7.2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1. The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
8.2. Generally this will be for the duration of your employment and 6 years post employment. We will keep data for unsuccessful candidates for 6months.
8.3. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

9. Accountability and Record-Keeping

9.1. The Human Resources Department is assigned by the Company to manage data and data protection issues.

9.2. The Human Resources Department shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10. Rectification of Personal Data

10.1. Employee data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

10.2. The Company shall rectify the personal data in question, and inform the employee data subject of that rectification, within one month of the employee data subject informing the Company of the issue. The 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 informed.

10.3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

11. Erasure of Personal Data

11.1. Employee data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

- the employee data subject wishes to withdraw their consent to the company holding and processing their personal data;
- the employee data subject objects to the company holding and processing their personal data (and there is no overriding legitimate interest to allow the company to continue doing so) (see section 18 of this policy for further details concerning the right to object);
- the personal data has been processed unlawfully;
- the personal data needs to be erased in order for the company to comply with a particular legal obligation.

11.2. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the employee data subject informed of the erasure, within one month of receipt of the employee data subject's request. The 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 informed.

11.3. In the event that any personal data that is to be erased in response to an employee data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

12. Data Protection Impact Assessments

12.1. The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of employee data subjects under the GDPR.

12.2. Data Protection Impact Assessments shall be overseen by the Human Resources Department and shall address the following:

- the type(s) of personal data that will be collected, held, and processed;
- the purpose(s) for which personal data is to be used;
- the Company's objectives;
- how personal data is to be used;
- the parties (internal and/or external) who are to be consulted;
- the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- risks posed to employee data subjects;
- risks posed both within and to the Company; and
- proposed measures to minimise and handle identified risks.

13. Sharing your personal data

13.1. Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

13.2. We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

13.3. Legitimate activities may include:

- storing personal data on our cloud based HR system;
- processing payroll;
- providing benefits such as pension, health cover and accident and life cover;
- booking flights and accommodation;
- booking training courses, seminars, networking events etc.;
- promoting the Company on social media or on our website;
- and for any other reason which we may notify you of from time to time.

13.4. The Company may transfer your data to countries outside the European Economic Area when utilising online tools such as Smartsheet or Align but will ensure that appropriate safeguards are in place.

14. How to deal with data breaches

14.1. We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

14.2. If you are aware of a data breach you must contact the Human Resources Department immediately and keep any evidence you have in relation to the breach.

15. Data Breach Notification

15.1. All personal data breaches must be reported immediately to the Human Resources Department.

15.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of employee data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Human Resources Department must ensure that the Information Commissioner's Office is informed of the breach

without delay, and in any event, within 72 hours after having become aware of it.

15.3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under clause 17.2) to the rights and freedoms of employee data subjects, the Human Resources Department must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.

15.4. Data breach notifications shall include the following information:

- the categories and approximate number of employee data subjects concerned;
- the categories and approximate number of personal data records concerned;
- the contact details of the Human Resources Department (or other contact point where more information can be obtained);
- the likely consequences of the breach; and
- details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

16. Organisational Measures

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

- all employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
- only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- all employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- all employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- all employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- all personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

- the performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- all employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- all agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and
- where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

17. Subject access requests

17.1. Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Human Resources Department who will coordinate a response.

17.2. If you would like to make a SAR in relation to your own personal data you should make this in writing to the Human Resources Department. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

17.3. There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

17.4. If you have a SAR, have any questions or have a complaint, please contact Human Resources Department.

18. Your data subject rights

18.1. You have the right to information about what personal data we process, how and on what basis as set out in this Policy.

18.2. You have the right to access your own personal data by way of a subject access request (*see above*).

18.3. You can correct any inaccuracies in your personal data. To do you should contact the Human Resources Department.

18.4. You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Human Resources Department.

18.5. While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Human Resources Department.

18.6. You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

18.7. You have the right to object if we process your personal data for the purposes of direct marketing.

18.8. You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

18.9. With some exceptions, you have the right not to be subjected to automated decision-making.

18.10. You have the right to be notified of a data security breach concerning your personal data.

18.11. In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Human Resources Department.

18.12. You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

This Policy has been approved and authorised by:
Name: Roscoe Price
Position: Managing Director
Date: 6th October 2021
Due for Review by: 6th October 2022
Signature: