MOMENTUM

TRAINING AND CONSULTANCY

GDPR

Policy

Data Protection

Introduction

This Policy sets out the obligations of the Company regarding data protection and the rights of its employees (in this context, “employee data subjects”) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”)

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.

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.

The Data Protection Principles

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

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

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.

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

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.

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.

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.

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object.

Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure 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 if at least one of the following applies**:**

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- Processing is necessary for performance of the data subject contract, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;

If the personal data in question is “special category data” otherwise known as “sensitive personal data” at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary for carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant

to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes personal data. This includes:

- Personal data collected directly from employee data subjects
- Personal data obtained from third parties.

The specific purposes for which the Company collects, processes, and holds such personal data are set out in this policy. (or for other purposes expressly permitted by the GDPR).

Employee data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

Adequate, Relevant, and Limited Data Processing

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.

Accuracy of Data and Keeping Data Up-to-Date

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.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. Inaccurate data will be updated without delay.

Data Retention

The Company shall not keep personal data for any longer than is necessary.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against

accidental loss, destruction, or damage.

Accountability and Record-Keeping

The Company's Data Protection Officer is Simon Watts, Owner and proprietor, simonwatts@groupmomentum.net.

The Data Protection Officer shall be responsible, working together with the HR Department for overseeing the implementation of this Policy and for monitoring compliance with this Policy, other relevant policies, GDPR and Data Protection Legislation.

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company, and the categories of employee data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for any new projects which encompass personal data of data subjects and a possibility to result in the rights and freedoms of employee data subjects under the GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The personal data that will be collected, held, and processed;
- The purpose 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.

Keeping Data Subjects Informed

The Company shall provide relevant information to the Data Subject, including but not limited to the following:

- Employee data subjects will be informed of the purpose of data collection at the time of collection; and
- Where personal data is obtained from a third party, the relevant employee data subjects will be informed of its purpose.

The following information shall be provided:

- Details of the Company including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed and the legal justification;
- Legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the employee data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Details of data retention;
- Details of the employee data subject's rights under the GDPR;
- Details of the employee data subject's right to withdraw their consent to the Company's processing of their personal data;
- Details of the employee data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Subject Access

Employee data subjects may make subject 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 personal data, and why.

Employees wishing to make a SAR should do using a Subject Access Request Form,

sending the form to the Company's HR Manager at julie@groupmomentum.net.

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the employee data subject shall be informed.

All SARs received shall be handled by the Company's HR Manager.

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 supplied to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

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

The Company shall rectify in a reasonable period of time. Data Subjects will be informed of progress in the event of a complex request.

Any affected personal data disclosed to third parties will be noted and the company shall be informed of any rectification to be made.

Erasure of Personal Data

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);
- 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;
- 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 a reasonable period of time. Complex requests may take longer, but the Data Subject will be informed;
- Where applicable the Company will notify any third-party data processors of an individual's request for erasure unless it is impossible or would require disproportionate effort to do so.

Restriction of Personal Data Processing

Employee data subjects may request that the Company ceases processing the personal data it holds about them. If an employee data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

Where application the Company will notify any third-party Data Processors of the restriction unless it is impossible or would require disproportionate effort to do so.

Personal Data

The Company holds personal data that is directly relevant to its employees. That personal data shall be collected, held, and processed in accordance with employee data subjects' rights and the Company's obligations under the GDPR and with this Policy. Details of the information the Company holds can be found in our Privacy Notice.

Health Records

The Company holds health records on all employee data subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In most cases, health data on employees falls within the GDPR's definition of special category data. Any data relating to employee data subjects' health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data No special category personal data will be collected, held, or processed without the relevant employee data subject's express consent.

Health records shall be accessible and used only by the HR Department, Directors and Direct Line Management (If necessary for employee wellbeing), and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company**,** except in exceptional circumstances where the wellbeing of the employee data subject(s) to whom the data relates is at stake.

Health records will only be collected, held, and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

Employee data subjects have the right to request that the Company does not keep health records about them. All such requests must be made in writing and addressed to Julie Gosling at julie@groupmomentum.net

Benefits

In the event that employee data subjects are enrolled in a benefit scheme (Company pension for example) it may be necessary to share personal data with the benefit provider.

Prior to the collection of such data, employee data subjects will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in

which it will be processed.

The Company shall not use any such personal data except insofar as is necessary in the administration of the relevant benefits schemes.

Employee Monitoring

The Company may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

Monitoring will only take place if the Company considers that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Company's obligations under the GDPR.

The Company shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using Company equipment or other facilities including, but not limited to, Company email, the Company intranet, or a virtual private network ("VPN") service provided by the Company for employee use.

Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data (including, but not limited to, personal data relating to employees):

- All emails containing personal data will be password protected, and passwords sent to the recipient
- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted
- Where personal data is to be transferred in hardcopy form it should be passed

directly to the recipient

- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data (including, but not limited to, personal data relating to employees):

- All electronic copies of personal data should be stored securely using passwords
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically should be backed up by the Company shared drive with backups stored at Momentum Head Office. All backups are password protected.
- No personal data should be stored on any personal mobile device, whether such device belongs to the Company or otherwise without the formal written approval of Simon Watts (contact details featured earlier in the policy), and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR. Due diligence shall be completed by the Company.

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason, it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Simon Watts.

- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Simon Watts;
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

Data Security - IT Security

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

- Passwords should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. They must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Passwords shall not be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. Forgotten passwords will be reset via the IT department;
- All software shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates within a reasonable period of the update becoming available and
- No software may be installed on any Company-owned computer or device without the prior approval of the IT Department.

Organisational Measures

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.

Transferring Personal Data to a Country Outside the EEA

The Company does not transfer data outside of the EU or EEA

Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Officer.

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, the Data Protection Officer 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.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of employee data subjects, the Data Protection Officer must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.

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 name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- 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.

Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Next up date: 25-05-2021

MOMENTUM

TRAINING AND CONSULTANCY