EMPLOYEE PRIVACY POLICY

WHAT IS THE PURPOSE OF THIS DOCUMENT?

Momentum Instore Limited (referred to in this document as "we" or the "Company") is committed to protecting the privacy and security of your personal information.

This privacy policy includes privacy notices and describes how we collect and use personal information about you during and after your working relationship with us, in accordance with applicable data protection laws and the EU General Data Protection Regulation (*EU 2016/679*) (GDPR).

It applies to all employees of the Company. This privacy policy does not form part of any contract of employment or other contract to provide services.

It is important that you read this Policy, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

CONTACT DETAILS

The Company's contact details are:

> Momentum Instore Limited, Beechwood Court, Springwood Way, Tytherington Business Park, Tytherington, Macclesfield, SK10 2XG.

Enquiries regarding this Policy, see Contact Us at the end of this document.

The Company is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you.

GDPR AND DATA PROTECTION PRINCIPLES

GDPR, which takes effect from 25 May 2018, will establish a single pan-European law for data protection and will enable individuals to better control their personal data, regardless of where this data is sent, stored or processed.

The Company has to comply with the provisions of GDPR when keeping personal data about our employees in a computer or in certain filing systems and when we obtain, use, disclose or otherwise process such data.

The Company collects and processes personal data relating to its employees to manage the employment relationship. The Company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

- We are required to comply with data protection law and principles, which means that your personal data will be:
- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

We collect and use the following kinds of information:

- Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).
- Special categories of personal data. GDPR describes the following types of personal data as 'special categories of personal data': information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sexual life (or sexual orientation), genetic or biometric data] and commission or alleged commission of any criminal offence. The Company needs to handle some of these special categories of sensitive personal data and other types of personal data about our employees in the ways described below in this Policy.

DATA PRIVACY MANAGER

The Data Privacy Mangers for the business are:

Danielle Dixon and Mike Lockey

The Data Privacy Managers will inform and advise on data protection and GDPR, monitor compliance within the organisation, cooperate and liaise with the ICO and be the point of contact for data subjects.

The Data Privacy Manager's contact details are: GDPR@momentuminstore.com.

WHAT PERSONAL DATA DO WE PROCESS?

We collect, store and process a range of personal information about you. This includes the following categories of personal information about you:

CONTACT

- Your name, address and contact details, including email address and telephone number

IDENTITY

- information about your marital status, next of kin, dependants and emergency contacts;
- date of birth and gender;
- information about your nationality and entitlement to work in the UK;

EMPLOYMENT TERMS AND HISTORY

- the terms and conditions of your employment, including your start date;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;

PERFORMANCE

- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence; and
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence.

TECHNICAL

- details held at DVLA of your driving license (which has been explicitly granted by you), details of the vehicle you use for work purposes (if you are in receipt of a car allowance), and your certificate of insurance showing cover for business use;

FINANCIAL

- details of your bank account and national insurance number;
- information about your remuneration, including salary and entitlement to benefits such as pensions or insurance cover.

We may also collect, store and process various “special categories” of more sensitive personal information. These are detailed further below under the heading “Special Categories of sensitive data”:

MEDICAL, HEALTH AND SICKNESS

- information about medical or health conditions, including whether or not you have a disability for which we need to make reasonable adjustments;
- information relating to leaves of absence, which may include sickness absence or family related leaves

OTHER SENSITIVE

- information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation
- criminal convictions records

HOW WE COLLECT YOUR PERSONAL INFORMATION

We may collect this information in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

In some cases, we may collect personal data about you from third parties, such as references supplied by former employers and information from employment background check providers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

Data will be stored in a range of different places, including in your personnel file which is stored securely in the HR Office, in the organisation's HR/Payroll folders/software such as Payroll Sage and in other IT systems (including the organisation's email system). Data will be held in both hard format and electronically.

Records may also be kept in places other than the employment file. For example, the HR department may keep central records and managers may also hold some records about an employee.

HOW WE USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances (each of these circumstances can also be referred to as a “basis” of processing:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be less common:

1. Where we need to protect your vital interests (or someone else’s interests).
2. Where it is needed in the public interest or for official purposes.
3. 3 Where we have obtained your consent.

We need to process the categories of information in the list above (see *Paragraph* headed "What personal data do we process?") on one or more of the following legal grounds:

- allow us to **perform our employment contract** with you. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements; and/or
- ensure that we are **complying with our legal obligations**. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled; and/or
- to protect the **vital interests** of the employee or another person; and/or
- pursue **legitimate interests** of our own or those of third parties before, during and after the end of the employment relationship, provided your interests and fundamental rights do not override those interests.
    - Our **legitimate interests** would include, for example: to detect and prevent fraud and crime; administrative purposes; performance and delivery of our services to customers; reporting potential crimes to relevant authorities; intra group transfers; employee administration, operations and recruitment; ensuring network, information and system security; participate and comply with industry watch-lists and industry self-regulatory schemes; corporate operations and due diligence (reporting of management information, operation of financial/risk/credit models, back office operation, managing third party service providers, corporate reorganisations); bringing or responding to legal claims or proceedings to protect the Company's tangible or intangible assets or interests.

We have set out below, in a table format, a description of all the ways and situations we will process your personal data, and which lawful basis we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Purpose/Activity	Type of Data *More detail about each type of data listed in this column below are explained under "What Personal Data do we process?"*	Lawful basis for processing including basis of legitimate interest
Make a decision about your recruitment or appointment.	Contact Identity Employment Terms and History Performance Technical Financial Other Sensitive	Processing personal data for this purpose is necessary for our legitimate interest. Where we have obtained your clear consent to process personal data for this purpose, consent shall be the basis for processing.

Determine the terms on which you work for us.	Contact Identity Employment Terms and History Technical Financial	Processing personal data for this purpose is necessary for our legitimate interests (employee administration, operations and recruitment).
Checking an employee's entitlement to work in the UK.	Contact Identity	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations and is necessary for our legitimate interests (employee administration, operations and recruitment).
Provide you with a contract, pay you in accordance with your employment contract/the law and administer benefit, pension and insurance entitlements. *Note:* An employee may be asked to provide the following sorts of information when applying to join the pension, life assurance or medical scheme (if applicable) – details of beneficiaries, medical history and family medical history. The employee can provide this directly to the scheme provider. The Company will not want access to medical information provided to the scheme provider other than in exceptional circumstances. If such circumstances arise (for example, if there is an allegation of dishonesty) the Company will seek employee consent before asking for access unless the law allows the Company to do otherwise.	Contact Identity Employment Terms and History Performance Technical Financial Medical, Health and Sickness	Processing personal data for these purposes is necessary to perform the employment contract and for the Company to comply with its legal obligations.
Ensure effective general HR and business administration, maintain accurate up-to-date employment records including records of employee contractual and statutory rights and contact details including details of who to contact in the event of an emergency.	Contact Identity Employment Terms and History Performance Technical Financial	Processing personal data for these purposes is necessary to perform the employment contract and for the Company to comply with its legal obligations and to protect the vital interests of the employee.

Note: When an employee starts work, details of an emergency contact and your home and mobile telephone numbers will be requested. The Company might call an employee's home or mobile telephone number in any situation where this might be helpful, for example, to ask about a work related matter when the employee is off sick.	Medical, Health and Sickness Other Sensitive	
Business management and planning, including accounting and auditing.	Contact Employment Terms and History Performance Financial	Processing personal data for these purposes is necessary to perform the employment contract, for the Company to comply with its legal obligations, for our legitimate interests (corporate operations and due diligence; employee administration, operations and recruitment) and to protect the vital interests of the employee.
Carry out recruitment and promotion processes. *Note:* Following the recruitment process, the Company will keep all relevant documents and records, such as an employee's CV, application form, application letters, references and interview notes. These documents and records are put on the employee's employment file and might be used for a variety of purposes including obtaining contact details, promotion etc.	Contact Identity Employment Terms and History Performance Financial	Processing personal data for these purposes is necessary to perform the employment contract, to comply with legal obligations and for our legitimate interests (employee administration, operations and recruitment).

Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace. *Note:* The Company keeps records relating to grievances raised by employees and may take notes of any conversations or meetings in which concerns are raised. This is to ensure that the Company is managing the employee properly and complying with its duties. Records and documents relating to any suspected disciplinary matter are also kept on employment files. After warnings have expired in accordance with the Disciplinary Procedure, they are not destroyed. They are kept on the employment file, and will not be used in determining the severity of any subsequent disciplinary penalty but are kept in case the Company needs to refer to them for other purposes (e.g. if a dispute arises over whether an employee was made aware of the inappropriateness of particular conduct or for legal proceedings).	Contact Employment Terms and History Performance Technical Financial Other Sensitive	Processing personal data for these purposes is necessary to perform the employment contract and for the Company to comply with its legal obligations.
Operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes. *Note:* During employment, we are likely to build up records about an employee in order to manage work and performance which will be kept on the employee's employment file and Performance Hub (online appraisal system). For example, the Company keeps copies of appraisals, notes of any meetings about an appraisal and reports from line-managers. The Company also keep information relating to work or performance if relevant to recent or future employment decisions.	Contact Employment Terms and History Performance Technical Financial	Processing personal data for these purposes is necessary to perform the employment contract, to comply with our legal obligations and for our legitimate interests (employee administration, operations and recruitment).

Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled. *Note:*The Company keeps absence records on our HR and Payroll software and may collect records of employees' starting, finishing and working times, particularly when considered appropriate for managing work, attendance or performance or in order to comply with the Working Time Regulations or other laws. The Company generally keeps records of any special leave (e.g. compassionate leave or jury service) in order to manage attendance levels. Reasons for such leave (e.g. death of relative) may also be recorded on your employment file	Contact Employment Terms and History Performance Financial Medical, Health and Sickness	Processing personal data for these purposes is necessary to perform the employment contract, for the Company to comply with its legal obligations and for our legitimate interests (employee administration, operations and recruitment).
Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.	Contact Identity Employment Terms and History Financial Medical, Health and Sickness	Processing personal data for these purposes is necessary to perform the employment contract, for the Company to comply with its legal obligations and for our legitimate interests (employee administration, operations and recruitment).
Obtain and keep a record of employee medical conditions and occupational health/GP advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled. *Note:* Throughout employment, we are likely to gain additional information about an employee's	Contact Identity Employment Terms and History Performance Technical Financial Medical, Health and Sickness	Processing personal data for these purposes is necessary to perform the employment contract, for the Company to comply with its legal obligations and to protect the vital interests of the employee or another person. **Special Categories and health or medical conditions**: Some special categories of personal data, such as information about health or medical conditions, is processed for the purposes and is necessary for the

health. Such information may come from the employee health questionnaire, fit notes or medical reports, return to work forms, from self-certification forms, from what is told to the Company and from the observations of colleagues. It may also come from medical reports or tests requested by the Company. The Company uses such information about health for the purposes of managing attendance and performance, administering pay and benefits, judging capacity to work and complying with our duties towards employees. Such information is likely to be kept on an employee's employment file. If an employee has particular concerns over who may have access to any specific information relating to his/her health please discuss this with a member of the HR Department.		purposes of carrying out the obligations and exercising specific rights of the Company or the employee in the field of employment law (such as those in relation to employees with disabilities) and to protect the vital interests of the employee or another person (see further under "Special Categories of Other Sensitive data").
Obtain/provide references on request for current or former employees.	Contact Employment Terms and History Performance Technical Financial Medical, Health and Sickness Other Sensitive	Processing personal data for this purpose is necessary to perform the employment contract, to comply with legal obligations and for the Company's legitimate interests (employee administration, operations and recruitment).
Respond to and defend against legal claims.	Contact Employment Terms and History Performance Technical Financial Medical, Health and Sickness Other Sensitive	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations and for the Company's legitimate interests (to bring or respond to legal claims or proceedings to protect the Company's tangible or intangible assets or interests).
Gather evidence for possible grievance or disciplinary hearings.	Contact Employment Terms and History Performance Technical Financial	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (to bring or respond

	Medical, Health and Sickness Other Sensitive	to legal claims or proceedings to protect the Company's tangible or intangible assets or interests).
Education, training and development requirements.	Contact Employment Terms and History Performance	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (employee administration, operations and recruitment).
Deal with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	Contact Identity Employment Terms and History Performance Technical Financial Medical, Health and Sickness	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (to bring or respond to legal claims or proceedings to protect the Company's tangible or intangible assets or interests).
Complying with health and safety obligations.	Contact Employment Terms and History Technical Medical, Health and Sickness	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations and performance of the employment contract.
To prevent fraud.	Contact Identity Employment Terms and History Technical Financial Medical, Health and Sickness Other Sensitive	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (to detect and prevent fraud and crime).
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	Contact Employment Terms and History Performance	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (employee administration, operations and recruitment).

Ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	Contact Employment Terms and History	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (ensuring network, information and system security).
Conduct data analytics studies to review and better understand employee retention and attrition rates.	Contact Employment Terms and History Performance Financial	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (employee administration, operations and recruitment).
Equal opportunities monitoring.	Contact Employment Terms and History Performance Financial	Processing personal data for this purpose is necessary for the Company to comply with its legal obligations, performance of the employment contract and for the Company's legitimate interests (employee administration, operations and recruitment)
Check criminal records.	Contact Identity Employment Terms and History Technical Other Sensitive	Processing personal data for this purpose is necessary for the performance of the employment contract, to comply with legal obligations, to protect the Company's legitimate interests (employee administration, operations and recruitment) and to protect the vital interests of the employee or another person.

Criminal Records: We will only use information relating to criminal convictions where the law allows us to do so and in accordance with GDPR. This will usually be where such processing is necessary to carry out our legal obligations. Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

The employee will be asked to detail any unspent criminal convictions on their HR Data form. If the Company learns (from any source) that an employee has been convicted or is suspected of a criminal offence, the Company will use this information only in limited circumstances. For example, the Company may use it for disciplinary purposes if it is considered that it may affect the employee's ability to do his/her job or the Company's reputation.

Health records: If an employee has particular concerns over who may have access to any specific information relating to his/her health please discuss this with a member of the HR Department or our Data Privacy Managers at GDPR@momentuminstore.com.

IF YOU FAIL TO PROVIDE PERSONAL INFORMATION

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

CHANGE OF PURPOSE

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

SPECIAL CATEGORIES OF SENSITIVE DATA

”Special categories” of sensitive personal information (some of which have been mentioned above under the headings “The kind of information we hold about you” and “How we use information about you”) require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

OUR OBLIGATIONS AS AN EMPLOYER

We will use your sensitive personal information in the following ways:

- information about your nationality to comply with employment and other laws;

- information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws
- information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

DO WE NEED YOUR CONSENT?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

MONITORING

The Company may carry out periodic checks on use of the email system and/or internet sites visited and reserves the right to monitor, retrieve and review employees' emails. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

The Company may monitor, and wherever necessary, review the history of communications made via any of its Information Technology and Telecommunications (ITT) systems. This includes access to the Internet via the Company's systems.

The purposes of this monitoring is to ensure that (i) the Company's ITT systems are used primarily to carry out the business of the Company and not excessive personal use, (ii) these systems are not being used for unlawful purposes and employees are complying with Company's ITT policies and the Company's systems (iii) system capacity is sufficient for the needs of the business.

The content of individual communications will be monitored only where necessary and justifiable, for example, if one employee is suspected of breach of this or another Company policy or if an employee is absent and e-mails need to be checked for work purposes. However, you should be aware that such monitoring may take place and that the content of your communications using the Company's ITT systems cannot therefore be regarded as completely confidential. You should therefore consider whether e-mail is the most appropriate method of communication for your personal purposes.

Wherever possible monitoring will be:

- Done automatically by our computer systems or otherwise by an appropriate member of the IT team and/or Line Manager and/or
- Limited to the assessment of traffic and/or
- Taken in the form of spot checks or audits rather than be carried out continuously and/or
- Targeted at areas of highest risk or where a particular problem is indicated

ACCESS TO DATA

In order for the Company to carry out the points listed above (under "How we use information about you"), some of your information will be shared internally on a need to know basis. This includes with members of the HR, Recruitment and Payroll team, your line manager, managers in the business area in which you work and IT/H&S/Fleet staff if access to the data is necessary for the performance of their roles. Employees should be assured that access to held information is restricted on a need to know basis.

If your role requires the Project Teams to plan your working schedule, for example if you are a Permanent Installer, the Project Teams may need to access some of your personal data for scheduling, travel and accommodation purposes. For example, they must know your address for journey planning and sending you project information. Processing personal data for this purpose is necessary to perform the employment contract.

THIRD PARTIES

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

We share your data with third parties in order to provide pre-employment references from other employers and obtain employment background checks from third-party providers.

We also share your data with third parties that process data on our behalf, in connection with payroll, the provision of benefits and the provision of occupational health services, IT services. For example, your personal data may be shared with:

- NEST (workplace pension scheme) in order to administer your pension entitlements. Processing personal data for this purpose is necessary to perform the employment contract and for the Company to comply with its legal obligations.
- Drivercheck and Europcar in order to hire you a vehicle, as we must ensure you are qualified to drive and covered under our insurance policy. By driving one of our hire vehicles you understand that any fines you incur will be your responsibility and as such we may also need to share your name with Parking Fine Companies for them to pursue this with you. Processing personal data for these purposes is necessary to perform the employment contract and for the Company to comply with its legal obligations.
- HMRC and the Police if the Company receives any such request in writing. Managers dealing with these requests will confirm that the request has come from a trusted party before any details are disclosed and will only send relevant need to know information. We may be required to share information when the Company is in situations where there is a statutory duty or Court Order requiring the information to be shared. Processing personal data for these purposes is necessary for the employer to comply with its legal obligations.

If you are a field based employee and/or carry out work on site in retail stores:

- your address and phone number may be shared with our Uniform provider to enable the company to deliver your uniform to you and the courier Company may need to contact

you to facilitate the delivery. Your address may also be shared with the Project Teams to send you project information via post. Processing personal data for these purposes is necessary to perform the employment contract and to protect our legitimate interests.

- we may share your name with clients prior to a project you are working on so they know who to expect on site for operational and health and safety reasons. Processing personal data for this purpose is necessary to perform the employment contract, to perform legal obligations and to protect the vital interests of the employee.
- Project Teams may need to share your passport details when applying for permits/access to store. For example, if you are working at an airport it would be shared with the British Airport Authority. Processing personal data for this purpose is necessary to perform the employment contract, to comply with legal obligations and for our legitimate interests.
- Project Teams may need to share your name with Priority & Hotels to confirm accommodation bookings and your passport details with other travel providers (airlines, train operators, ferries etc.) where travel/accommodation is required to be booked as part of a project. Processing personal data for this purpose is necessary to perform the employment contract and for our legitimate interests.
- Project Teams may need to share your contact number with other employees/workers who are working on the same site as you so you can coordinate times to meet, arrange lifts etc. Processing personal data for this purpose is necessary to perform the employment contract and for our legitimate interests (performance and delivery of our services to customers).

We may share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for IT or system operation or maintenance support and hosting of data.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business but will only do so under strict conditions of confidentiality and as permitted by GDPR. We may also need to share your personal information with a regulator or to otherwise comply with the law.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We will not transfer your data to countries outside the European Economic Area without your further explicit consent.

PROTECTION OF DATA

We treat the security of your data with the utmost importance. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed in an unauthorized way. The ability to access data is restricted to employees, agents, contractors and other third parties who have a business need to know. Some of the key measures in place to ensure this include:

- The ability to access data is restricted on a need to know basis. AD security groups are used to permission sensitive server data and Access Control Groups are used on our extranets.
- SSL certificates are used on all our sites as standard, to ensure data in transit is encrypted
- All Insite system data is subject to back-up at transaction level throughout each day, and full back-up is performed each morning. All server data is backed up using Veeam using the 3-2-1 methodology and copies stored offsite.
- Insite SQL servers are mirrored, with automatic failover (Microsoft Azure servers based in the EU)
- Sophos End Point Protection software protects all employee PCs\Laptops
- Server based data sits behind a WatchGuard M370 firewall with IDP & an active subscription
- AD policy is that all user account lockout automatically after 3 failed password attempts. Accounts can only be unlocked by a member of the IT team. Network passwords have to be at least 8 characters in length and contain at least one uppercase character and a number. These expire every 30 days.
- All laptops and mobile devices are encrypted and the use of non-encrypted removable storage media is prohibited (via a Sophos Device Control policy)
- A clean desk policy is in place

Where we engage third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

DATA RETENTION PERIODS

We will hold personal data about you for the duration of your employment.

What Happens If You Leave?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your

personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you are no longer an employee, worker or contractor of the Company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

If the Company provides a reference about you, our practice is to ask the recipient to keep it confidential. In preparing a reference the Company may use any records or information held on the employee for this purpose and any reports from managers or others taken specifically for this purpose.

We do not object to managers and colleagues providing references in a personal capacity but, if they choose to do so, we will not have any responsibility for the information in that reference.

Employment files and payroll details will be reviewed to check for inaccuracies, update old information and remove information that is no longer required.

DATA SUBJECT RIGHTS

As a data subject, under certain circumstances, you have a number of rights:

- Request access - You can access and obtain a copy of your data on request (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Correction - You can require us to change incorrect or incomplete data we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Erasure - You can require us to delete or stop processing your personal data, for example where the data is no longer necessary for the purposes of processing. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing - You can object to the processing of your personal data where the organisation is relying on its legitimate interests (or those of a third party) as the legal ground for processing;
- Request the restriction of processing - You can request the restriction of processing. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- Transfer request - You can request the transfer of your personal information to another party;
- Automated Decision- Making
  You have the right not to be subject to a decision based solely on automated processing (Automated Decision-Making), which produces either legal or other significant effects. Automated Decision-Making takes place when an electronic system uses personal information to make a decision without human intervention. Examples of this are:

- Automatic rejection of candidates when recruiting online if they do not have certain qualifications
- A 'trigger' in a procedure for sickness absence or disciplinary action
- Bonus decision made on attendance data

We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

All data subject access requests from individuals to view their data being held by Momentum Instore should be addressed to GDPR@momentuminstore.com. The Company will firstly ask you to complete a Subject Data Access Request form for the purposes of properly verifying the identity of the individual making the request, ensuring it is lawful for us to provide the individual with the requested information and to understand specifically what data is being requested. The Company will then supply the electronic information requested within 1 month from the date of request for standard information requests. More complex information requests may take up to 3 months.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing at GDPR@momentuminstore.com.

The Company recognises an individual's "Right to be Forgotten", and such requests should be sent to GDPR@momentuminstore.com.

RIGHT TO COMPLAIN

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner. Contact details can be found at the ICO website: https://ico.org.uk.

NO FEE USUALLY REQUIRED

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

WHAT WE MAY NEED FROM YOU

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer at GDPR@momentuminstore.com. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

EMPLOYEES DUTIES

To help the Company keep accurate information, you must tell us about changes to contact, payroll or other personal details. You also have a role to play in helping the Company meet its obligations to handle personal data relating to other employees/workers in accordance with GDPR.

If you receive a request for disclosure of information about another employee/worker from someone not employed by the Company, you must be careful. You should take all reasonable steps to establish the identity of the person seeking the information, obtain a written request or phone number and then pass the request to a member of the HR Department.

You must be aware of how you are handling Personal data – if someone is recognisable from the data then this is Personal Data, for example:

- Photographs
- Names
- Address
- Email Addresses
- Medical details or banking details

If you need to handle personal information relating to another employee/worker/client as part of your job, you should do so only as reasonably necessary for your job and take all reasonable steps to protect the security of that information. You should not be sharing data unless you have been authorised to do so. The examples below are where employee personal data may be being actively shared for operational reasons, subject to the processes and procedures required by the Company and notified to the relevant employees in the course of employment duties:

- Project Assistants share worker/sub-contractor Passport details (Name, Passport No, DOB) when applying for permits/access to store
- Project Teams and RMC share numbers of installers working on the same site together so teams can co-ordinate times to meet etc.

- Project Teams and Resource Managers will share worker names with clients so they know who to expect on site
- Resource Managers share drivers numbers with passenger's and passengers numbers with the drivers so they can organise lifts and they know who to pick up/who is picking them up and can make arrangements
- Resource Managers share workers names with Priority & Hotels, name/email/address with Europcar and passport details to other travel providers (airlines, train operators, ferries etc) where travel/accommodation is required to be booked as part of a project

If you have any saved documents which contain personal data these will need to be protected by a password and you must only keep essential/need to know information. Emails containing personal data will need to be protected (password protect the attachment and communicate the password separately) and if you are sending mass emails you must ensure you use Bcc (blind copy) so emails are not seen by all recipients. All personal data kept on a USB stick must be encrypted with passwords and you must ensure you have a passcode on your company mobile phone. If you lose your phone, laptop or USB stick this must be reported to IT immediately, so this can be reported (if we as a business haven't reported it within 72 hours of the data breach then we can be subject to a fine).

Employees must also use the confidential waste bins provided for disposing of documents containing personal data. Failure to do so could lead to a data breach and disciplinary action being taken against the employee.

If you have managerial responsibility for staff, you should be careful when collecting records about your staff, team or department. You must do so only as reasonably necessary for management purposes and must take all reasonable steps to protect the security of that information. If you are asked to give a reference about a current or previous employee, you should seek approval of the wording from the HR Department before sending it. You are not prevented from providing references in a personal capacity, but we will not have any responsibility for the information in that reference.

Employees in doubt about handling personal information relating to other employees should seek guidance. Accessing, keeping, disclosing or otherwise using records of other employees without authority is a serious disciplinary offence (and in some cases may constitute a criminal offence).

RESPONSE TO DATA BREACH

Responsibilities

All users including but not limited to; Employees, Workers, Contractors, Owners of Momentum Instore and any third party users have an obligation to be aware of, follow and comply with this procedure in the event of a personal data breach caused by themselves or another.

Once a breach has been reported by an Employee, Worker, Contractor, Owner of Momentum Instore or any third party, the organisation must comply with the procedures outlined below.

The Data Privacy Managers is responsible for ensuring this procedure is reviewed and updated in line with GDPR requirements.

Personal Data Breach

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. For example:

- access by an unauthorised third party
- sending data to an incorrect recipient
- losing computer devices which contain personal data
- alteration of personal data without permission

Procedure – Reporting a Breach Internally

Any user who negligently, intentionally, accidentally or otherwise causes a breach, should report this breach to The Data Privacy Managers or to their manager should the Data Privacy Managers be out of the office, by way of email detailing when the breach occurred, who the breach was made by, the full details of the breach, who the data subject is that the breach concerns and any other relevant information.

Any user who becomes aware of a breach whether by themselves, another individual or system etc. should report the breach in the same way.

No attempt should be made to mitigate the breach by any person unless advice has first been sought from the Data Privacy Managers or unless they have undertaken the relevant training which has authorised them to do so in the absence of this advice.

As soon as any person becomes aware of a breach, this must be reported as soon as possible but as a minimum, within 24 hours of becoming aware of the breach occurring.

A failure to report a breach in compliance with this procedure could result in disciplinary action for employees up to and including dismissal for Gross Misconduct.

A failure to report a breach in compliance with this procedure could result in the Company disposing of the services of any Worker, Contractor or other third party with or without notice.

CHANGES TO THIS PRIVACY POLICY

Changes to the privacy policy will be communicated with reasons for such changes (for example changes in law or changes in approach/uses).

CONTACT US

If you have any questions or queries regarding this policy please direct these to our Data Privacy Managers at GDPR@momentuminstore.com.

Momentum Instore

The contents of this Handbook are correct as at the time of production and as noted in the version control.

Please refer to HR for further information.