MOMENTUM INSTORE LTD - PROSPECTS, CLIENTS & SUPPLIERS PRIVACY POLICY

Last updated 23/05/2018

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, use and store personal information about you, before, 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 prospects, clients and suppliers on whom we collect, store and process personal data (referred to as data subjects). This privacy policy does not form part of any contract to provide or procure services.

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

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, SK10 2XG.

: 01625 569 200

(Registered in England under Company Number 2875057)

Data Privacy Manager

The Data Privacy Manager's role is to inform & advise on data protection and GDPR, monitor compliance within the organisation, cooperate & liaise with the ICO and be the point of contact for data subjects.

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

Changes to This Privacy Policy and your duty to inform us of changes

This version was last updated on 23rd May 2018. Changes to the privacy policy will be communicated with reasons for such changes (for example changes in law or changes in approach/uses).

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

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 prospects, clients and suppliers in electronic or paper based filing systems and when we obtain, use, disclose or otherwise process such data.

The Company collects and processes personal data relating to its prospects, clients and suppliers to manage the business relationship. The Company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

The Date We Collect About You

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).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

Momentum Instore

Data Type	Description	Prospects	Clients	Suppliers
Identity Data	Includes first name, last name, username or similar identifier, title, gender & social media links.	✓	✓	✓
Contact Data	Includes company billing address, delivery/store/branch address(s), email address and telephone numbers.	✓	✓	✓
Financial Data	Includes company bank account details and spend.	✗	✓	✓
Transaction Data	Includes details about payments to and from you or your organisation or business and other details of products and services you or your organisation or business have purchased from us (clients), or we have purchased from you (suppliers).	✗	✓	✓
Technical Data	Includes your login data (time, date, number of logins etc) you use to access our systems.	✗	✓	✓
Profile Data	Includes your system username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.	✓	✓	✓
Usage Data	Includes information about how you use our website, products and services (clients) and how we use your products and services (suppliers).	✓	✓	✓
Marketing and Communications Data	Includes your preferences in receiving marketing from us and your communication preferences.	✓	✓	✗

We also may collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific system feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

Momentum Instore

If You Fail to Provide Personal Data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

How is Your Personal Data Collected?

We use different methods to collect data from and about you including through:

- Direct interactions. You may give us your data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you/we provide when you/we:
    - register an interest in our/your products or services (e.g. via our website, at an exhibition or an advertisement etc.);
    - enter into a contract with us/you;
    - subscribe to our service or publications (e.g. blogs);
    - request marketing information to be sent to you;
    - complete a survey; or
    - give us some feedback.
- Automated technologies or interactions. As you interact with our website &/or systems (Insite), we may collect technical data about your equipment, browsing actions and patterns.
    - We collect this personal data by using cookies, and other similar technologies.

A cookie is a text file sent by a web server to a web browser, and stored by the browser. The text file is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser. We use two types of cookies – 'Strictly necessary cookies' and 'Analytical/performance cookies'.

We may send a cookie which may be stored on by your browser on your computer's hard drive. We may use the information we obtain from the cookie in the administration of this website, to improve the website's usability and for marketing purposes. We may also use that information to recognise your computer when you visit our website, and to personalise our website for you. Advertisers on our website may also send you cookies.

Most browsers allow you to refuse to accept cookies. This will, however, have a negative impact upon the usability of many websites, including this one.

We also use Google Analytics to analyse the use of this website. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to our website is used to create reports

about the use of the website. Google will store this information. For further details see Google's privacy policy and our own cookie policy, which is available on our website.

- **Third parties or publicly available sources.** We may receive personal data about you from various third parties and public sources as set out below:
    - **Technical Data** from the following parties:
        a. Emphasys - developer of Insite (based inside the EU)
        b. Google Analytics (based inside the EU)
        c. search information providers such as Google, LinkedIn, Facebook, Twitter etc. etc (based inside **or** outside the EU).
        (https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage https://support.google.com/analytics/answer/6004245)
    - **Contact, Financial and Transaction Data** about your business from providers of technical, payment and delivery services such as Experian (based inside the EU).
    - **Identity and Contact Data** about your business from publicly availably sources such as Companies House and the Electoral Register (based inside the EU).

How we Use Your Personal Data

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.
4. We may also use your personal information in the following situations, which are likely to be less common:
5. Where we need to protect your vital interests (or someone else's interests).
6. Where it is needed in the public interest or for official purposes.
7. Where we have obtained your consent.

The table below describes all the ways we plan to use your personal data, and which of the legal bases (see Glossary – Legal Bases) we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Momentum Instore

Note that we may process your personal data for more than one lawful basis depending on the specific purpose for which we are using your data. However, where we seek your consent to particular processing of your personal data, consent will be the legal basis for such processing. Please contact us if you need details about the specific legal basis we are relying on to process your personal data where more than one basis/ground has been specified:

Purpose / Activity	Type of data	Lawful basis for processing, including basis of legitimate interest
CRM System/Database: To keep you informed of our services for business-to business marketing in relation to prospects where we aren't currently engaged in a contract with you or your company and for existing clients who may be interested in additional services	Identity Contact Marketing and Communications Data	Necessary for our legitimate interests (to promote our products/services and grow our business) Where you are a sole trader, it is necessary to perform our contract with you Note that where we are required by applicable data protection laws to obtain your consent to contact you for marketing, we will also obtain such consent from you in the manner required by data such protection laws.
Proposal / Contract Documentation: To register you as a new customer / supplier	(a) Identity (b) Contact (c) Financial	Where you are a sole trader, performance of a contract with you Necessary for our legitimate interests (to promote, sell and deliver our products/services and grow our business;)

To process and deliver or receive services/products to/from your company including: (a) Fulfil a contract (b) Manage payments, fees and charges (c) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Where you are a sole trader, performance of a contract with you/us (b) Necessary for our legitimate interests (to recover debts due to us/you; to promote, sell and deliver our products/services and grow our business;)
To provide you with access to our online reporting and Estate Management Systems (Insite)	(a) Identity (b) Contact	Where you are a sole trader, performance of a contract with you Necessary for our legitimate interests (to promote, sell and deliver our products/services and grow our business;)
Business management, administration and planning, including accounting and auditing	(a) Identity (b) Contact (c) Financial (d) Transaction	Performance of a contract with you, Necessary for us to comply with our legal obligations, Necessary for our legitimate interests (corporate operations and due diligence; employee administration, operations and recruitment; to promote, sell and deliver our products/services and grow our business;).
Google Data Analytics: Conduct data analytics studies to review and better understand the performance of our website	(a) Technical (b) Usage	Necessary for the Company's legitimate interests(to promote, sell and deliver our products/services and grow our business;
Legal Disputes: Deal with legal disputes involving your company.	(a) Identity (b) Contact	Necessary for the Company to comply with its legal

	(c) Financial (d) Transaction (e) Profile	obligations, performance of contracts (where you are a sole trader) 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).
To develop &/or procure new products and services and to review and improve current products and services	(a) Financial (b) Transaction (c) Technical (d) Profile (e) Usage	Necessary for the Company's legitimate interests (to promote, sell and deliver our products/services and grow our business;
To facilitate the sale of one or more parts of our business or ownership of the Company	(a) Contact (b) Financial (c) Transaction (d) Profile (e) Usage	Necessary for the Company's legitimate interests (corporate operations and due diligence; corporate reorganisations; sale of the business or assets of the business carried out by us)
To monitor and to keep records of our communications with you and our staff	(a) Identity (b) Contact	Necessary for our legitimate interests (corporate operations, auditing and due diligence).

How we Store Your Personal Data

Data may be stored both electronically and in hard copy in a range of different places including:

- Our CRM system/database (on premise)
- Our ERP/financial system/database (on premise)
- Outlook / email (on premise & cloud based)
- Insite (cloud based)
- Secure server folders (on premise)
- Contracts & Proposal documents (on premise)

We may collect additional personal information in the course of contract activities throughout the period of our working relationship.

Momentum Instore

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.

Access to Data

In order for the Company to carry out the points listed above (under "How we use your personal data"), some of your information will be shared internally on a need to know basis. This includes with members of several different departments including:

- Sales & Marketing
- Installation and Merchandising project teams
- IT
- Finance

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 also share your data with third parties that process data on our behalf, in connection with outsourced system provision. For example, your personal data may be shared with:

- Emphasys – development and hosting provider for Insite (our client reporting and estate management system) and our two mobile apps, InTouch (data collection) and InSite (data reporting).
- Governmental and regulatory bodies such as HMRC & the Information Commissioners Office.
- Other organisations and businesses who provide services to us such as backup and server hosting providers, IT software and maintenance providers and suppliers of other back office functions.
- 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 or

possible sale or restructuring of the business (but will only do so under strict conditions of confidentiality and as permitted by GDPR)

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

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.

Data Security & Data Breach Notification

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. Active Directory ("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.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Data Retention Periods

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. Details of retention periods for different aspects of your personal information are available in our retention policy which information is available by request from our Data Privacy Manager (please send an email to gdpr@momentuminstore.com). 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 no longer have dealings with you (because for example you are no longer a client or supplier), a we will retain and securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations.

The Company may need to keep certain information to respond to and defend against legal claims for up to 6 years. We will review your personal data regularly during any retention period to ensure that it is still needed, is accurate and not excessive. Your personal information will be kept securely and in any event destroyed after 6 years (unless required by law to maintained for longer).

Your Legal Rights

As a data subject, under certain circumstances, you have a number of rights under data protection laws in relation to your personal data:

- 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;

DATA SUBJECT ACCESS REQUESTS

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.

RIGHT TO BE FORGOTTON

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

RIGHT TO COMPLAIN

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

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.

Momentum Instore

RIGHT TO WITHDRAW CONSENT

In the 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.

Glossary / Terms

GDPR - General Data Protection Regulation is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). ... GDPR is effective across the EU on May 25, 2018.

Data Controller - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Subjects - means an individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Lawful bases for data processing – The lawful bases we use for processing data, as set out in Article 6 of the GDPR are:

- Consent: the data subject has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract we have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legitimate interests: the processing is necessary for your legitimate interests of the legitimate interests of one of a 3rd party (unless there is a good reason to protect the individuals personal data which overrides those legitimate interests).
- Legal obligation: the processing is necessary to comply with the controller's legal obligations.
- Public interest: Where processing is needed in the public interest or for official purposes.

ICO – Information Commissioner's Office (https://ico.org.uk). The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Momentum Instore

Prospect (Sales Lead) – Potential customer or client qualified on the basis or their buying authority, financial capacity, and willingness to buy. The personal data of multiple data subjects may be held by us relating to a single customer or client.

Client – Customer or client for whom we are contractually engaged to provide and deliver a service(s) or have done work for in the past and are likely to do work for in the future. Multiple data subjects may be held by us relating to a single active customer or client.

Supplier (Vendor) – A person or company that provides goods &/or services to Momentum Instore. The personal data of multiple data subjects may be held by us relating to a single supplier.

Insite – Our Client reporting and Estate management portal, hosted and developed by or 3rd party partner, Emphasys.

ERP – Our Enterprise resource planning tool delivering integrated core business processes.

CRM – Our Customer relationship management tool used to store and analyse prospect and client data subjects and relationships.

App – Application (software) designed to work on a mobile or tablet. We operate an InTouch app (used by our filed teams to collect data) and an InSite app (used by our clients to report on their data.

AD – Active Directory ("AD") is a Microsoft technology that allows networks administrators to manage users, computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers.