Last Updated: June 27, 2022

This Data Processing Agreement ("Agreement") forms part of the agreement between Customer **(Customer)** and MSite **(Provider)** covering Customer's use of the Services (as defined below).

AGREED TERMS

1. Definitions and Interpretation

Business Purposes: the services to be provided by the Provider to the Customer and any other purpose specifically identified in ANNEX A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller: has the meaning given to it in section 6, DPA 2018.

Data Protection Legislation: means (i) the UK Data Protection Act 2018 (as amended and/or updated from time to time) ("DPA") and (ii) the UK General Data Protection Regulation ("UK GDPR") (as amended and updated from time to time);

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services;

Processing, processes, processed, process: any activity that involves the use of the Personal Data, including, but not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given to it in Clause 12.

Term: this Agreement's term as defined in Clause 10.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

2. Personal data types and processing purposes

2.1 The Customer and the Provider agree that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Service Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider shall promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Provider must comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires the Provider to process or disclose the Personal Data to a third-party, the Provider shall first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner under the Data Protection Legislation.

3.5 The Provider must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Provider's performance of this Agreement.

3.6 The Provider will only collect Personal Data for the Customer using a notice or method that the Customer specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of the Customer's identity, the purpose or purposes for which their Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. The Provider will not modify or alter the notice in any way without the Customer's written consent.

4. Provider's employees

4.1 The Provider will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable domestic law on all of the Provider's employees with access to the Personal Data.

5. Security

5.1 The Provider must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX B.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 The Provider will within 24 hours and in any event without undue delay notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

6.5 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Provider caused such, including all costs of notice and any remedy as set out in Clause 6.5.

7. Cross-border transfers of personal data

7.1 The Provider (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK without obtaining the Customer's prior written consent.

8. Subcontractors

8.1 The Provider may not authorise any third party or subcontractor to process the Personal Data.

8.2 Other than those subcontractors as set out in ANNEX A, the Provider may not authorise any other third-party or subcontractor to process the Personal Data.

8.3 Those subcontractors approved as at the commencement of this Agreement are as set out in ANNEX A. The Provider must list all approved subcontractors in Annex A and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.4 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider which contains terms substantially the same as those set out in this Agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.5 The Parties agree that the Provider will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

9. Complaints, data subject requests and third-party rights

9.1 The Provider shall, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2 The Provider shall notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider shall notify the Customer within 5 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider shall give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as the Provider retains any of the Personal Data in its possession or control (**Term**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination in order to protect the Personal Data will remain in full force and effect.

10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 30 days, either party may terminate on written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Provider will certify in writing to the Customer that it has deleted or destroyed the Personal Data within 30 days after it completes the deletion or destruction.

12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, [approved subcontractors], the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 12.1 (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Agreement and the Data Protection Legislation and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Annexes to this Agreement Annually to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least 90 days' notice, during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Personal Data.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach has occurred or is occurring, or the Provider is in material breach of any of its obligations under this Agreement or any of the Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, the Provider will:

(a) promptly conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 60 days.

13.4 At least once a year, the Provider will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a penetration testing assessment performed by a recognised third-party audit firm based on recognised industry best practices.

13.5 On the Customer's written request, the Provider will make all of the relevant audit reports available to the Customer for review, including reports relating to its Penetration Testing, Cyber Essentials and ISO/IEC 27001 certification. The Customer will treat such audit reports as the Provider's confidential information under this Agreement.

13.6 The Provider will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider's management.

14. Warranties

14.1 The Provider warrants and represents that:

(a) its employees, subcontractors and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.

16. Notice

16.1 Any notice given to a party under or in connection with this Agreement must be in writing and delivered to:

For the Customer: [CUSTOMER DATA PRIVACY CONTACT]

For the Provider: Jon Busby, Data Protection officer, jon.busby@msite.com

16.2 Clause 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This Agreement has been entered into on the date stated at the beginning of it.

ANNEX A Personal Data processing purposes and details

The Customer wishes to engage the services of the Provider to process personal data on his behalf under the terms and conditions of this contract

1. Subject matter and duration of the Contract

1.1. Subject matter

The Subject matter of the Agreement regarding the processing of data is the execution of the following services or tasks by the Provider as the Data Processor as follows:

The Customer is the Data Controller and uses Provider's online software solution "MSite" as a so-called Software as a Service (SaaS).

MSite provides, among other things, an integrated solution for workforce management, inductions, training, right to work checks, employee accreditation & reporting offering a fingerprint/face biometric construction site access control system that uses employee data to improve site safety and security.

Customer created content may relate to personal data of its employees and the employees or potential employees of its sub-contractor/client workforce.

2. Specification of Contract Details:

2.1. Nature and Purpose of the intended Processing of Data

The undertaking of the contractually agreed processing of personal data.

2.2. Type of Data

MSite Customers can configure MSite to store different types of personal data including but not limited to:

- Name
- Email address
- Address and address history
- Date and place of birth
- Nationality
- Gender
- Next of kin
- NI Number
- Passport information / Identification Documentation
- Employee Profile Image (Photo)
- Biometric data
- Health data
- Location data

- Thermal image temperature
- Equality and Diversity Information

2.3. Type of Data

The Subject Matter of the processing of personal data comprises the following data types/categories:

- Personal Master Data (Key Personal Data)
- Contact Data
- Disclosed Information (from third parties, e.g. Credit Reference Agencies or from
- Public Directories)
- Other Personal Data that the Customer/users insert when using MSite

2.4. Categories of Data Subjects

Employees, workers or contractors including subcontractors and/or suppliers of the Customer in its supply chain as instructed by the Customer.

The Categories of Data Subjects comprise:

- Employees of MSite Customer
- Employees of MSite Customer sub-contractors
- Potential employees of MSite Customer clients
- Sub-Contractors
- Employees of Potential Customers

3. Rectification, restriction and erasure of data

3.1. The Provider may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Customer, but only on documented instructions from the Customer or in accordance with the Commercial/Service Agreement. Insofar as a Data Subject contacts the Provider directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Customer.

3.2. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Provider in accordance with documented instructions from the Customer without undue delay.

4. Sub-Processors

4.1. MSite uses certain sub-processors to assist in providing it's services. A sub-processor is a third party data processor engaged by MSite who agrees to receive personal data intended for processing activities to be carried out (i) on behalf of MSite customers; (ii) in accordance with customer instructions.

4.2. The Provider may commission sub-processors according to this Contract or after prior written or documented consent from the Customer. The Customer agrees to the commissioning of the following sub-processors on the condition of a contractual agreement in accordance with GDPR Article 28 paragraphs 2-4:

Sub-Processor	Types of data Transferred	Purpose for the data transfer	Location
Amazon Web Services	All	Infrastructure as a Service provider	London, United Kingdom
Twilio	First name, Last name, Phone number	SMS Invite to employee to complete registration	USA
Loquate	Employee Postcode, Lodging Postcode	Travel distances to Site	United Kingdom
CITB Construction Training Register	Last name, DOB, NI number	Validate employee details	United Kingdom
Microsoft Azure	All – Pseudonymised	Statistical and analytical Dashboards & Reporting	London, United Kingdom

4.3. Provider is furthermore entitled to change the existing sub-processors with a new sub-processor providing equivalent services when:

4.3.1. The Provider informs the Customer of such outsourcing with appropriate advance notice; and

4.3.2. The subcontracting is based on a contractual agreement in accordance with GDPR Article 28 paragraphs 2-4.

4.4. The transfer of personal data from the Customer to the sub-processors and the sub-processors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

ANNEX B Security measures

Description of the technical and organisational security measures implemented by the Provider:

People Security

All MSite staff, not just a sub-set of staff, must pass stringent Criminal Record background checks and all staff complete GDPR training during the onboarding process and this training is refreshed annually.

Product Security

MSite is developed with a robust Privacy by Design (PbD) approach with data security the priority and centre of our platform architecture. MSite engineers perform internal security reviews before products are launched and MSite regularly performs third-party penetration testes. All data is Encrypted in Transit with MSite supporting TLS 1.2 to encrypt network traffic between the MSite web/mobile applications and MSite data centres. MSite secures your secrets using industry best practice methods to salt and repeatedly hash your credential before it is stored. Users can also add another layer of security to their account by using two-factor authentication (2FA) for the MSite console.

Datacentre Security & Compliance

MSite leverages AWS data centres for all production systems and customer data. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS. MSite (AWS) developers and administrators on the corporate network who need to access AWS cloud components in order to maintain them must explicitly request access through the AWS ticketing system. All requests are reviewed and approved by the applicable service owner. Approved AWS personnel then connect to the AWS network through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review.

Business Continuity / Disaster Recovery

Hosting our services on AWS gives MSite the ability to remain resilient even if one location goes down. AWS spans multiple availability zones, which allow MSite servers to remain resilient in the event of most failure modes, including natural disasters or system failures. MSite performs regular backups of customer data using Amazon S3 cloud storage. All backups are stored redundantly across multiple availability zones and encrypted in transit and at rest using strong encryption.