<sitekit>

DATA PROCESSING AGREEMENT

Between
[Client Name] [client address] (representing and acting on behalf of the “Data Controller”)

and
Sitekit Limited of Sitekit House, Broom Place, Portree, Isle of Skye, IV51 9HL (the “Data Processor”)

1 RECITALS

- In order to perform the Services on the Data Controller’s behalf, the Data Processor will require certain data to be made available to it by the Data Controller.
- Under the Data Protection Act 1998 and Regulation (EU) 2016/679 (the “General Data Protection Regulations”), the Data Controller is required to put in place an agreement between the Data Controller and any organisation which processes personal data on its behalf governing the processing of that data.
- The parties now wish to enter into this Agreement in order to regulate the provision and use of Personal Data that the Data Processor will be processing on behalf of the Data Controller.

2 AGREEMENT

2.1 DEFINITIONS AND INTERPRETATION

2.1.1 The following words and phrases used in this Agreement and the Schedules shall have the following meanings except where the context otherwise requires:

- “Data Controller” means the organisation that determines the purposes to which data is put and with whom it is shared, or in the case of a sub-processing agreement, an organisation authorised to act on the Data Controller’s behalf.
- “Master Contract” means the main contract between the Data Controller and Data Processor setting out the terms and conditions for the services to be provided by the Data Processor;
- "Data Subject" means an individual who is the subject of personal data;
- “Personal Data”, “Person Identifiable Data” or “PII” mean data which relates to a living individual who can be identified from that data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller or data processor. The conditions of processing personal data under this agreement are defined in Schedule A;
- “Sensitive Data” means data belonging to an individual which is regarded as confidential and sensitive under the Data Protection Act 1998 or falls into the “special categories” of data in GDPR. The conditions of processing sensitive data under this agreement are defined in Schedule A;
- “Services” means the services to be carried out by the Data Processor in the provision of a CMS system;
- “Consent” means permission for data processing and sharing, freely given by the data subject and conforming the Transparency principle set out in Regulation (EU) 2016/679 (the “General Data Protection Regulations”)

2.1.2 This Agreement shall continue in full force and effect for the same period as the Master Contract, unless terminated for breach by either party.

2.2 OBLIGATIONS OF THE DATA CONTROLLER

2.2.1 The Data Controller shall provide the Personal Data to the Data Processor together with such other information as the Data Processor may reasonably require in order for the Data Processor to provide the Services.

2.2.2 The instructions given by the Data Controller to the Data Processor in respect of the Personal Data shall at all times be in accordance with the laws of the United Kingdom.

2.2.3 In the configuration and operation of their CMS site(s), the Data Controller shall observe the Conditions for Processing set out in Schedule A below, and shall have sole responsibility for data protection and security if the conditions are not observed.

2.3 OBLIGATIONS OF THE DATA PROCESSOR

2.3.1 The Data Processor will process the Personal Data in compliance with applicable data protection regulations, including the Data Protection Act 1998 and Regulation (EU) 2016/679 (the “General Data Protection Regulations”).

2.3.2 The Data Processor undertakes that it shall process the Personal Data strictly in accordance with the Data Controller's instructions for the processing of that personal data.

2.3.3 The Data Processor will process the Personal Data for the purposes defined in Schedule C only.

2.3.4 The Data Processor will treat the personal data, and any other Information provided by the Data Controller as confidential, and will ensure that access to the Personal Data is limited to only those employees who require access to it for the purpose of the Data Processor carrying out the permitted processing and complying with its obligations under this Agreement.

2.3.5 The Data Processor will ensure that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data. The Data Processor will ensure that all such employees have undergone training in the law of data protection, their duty of confidentiality under contract and in the care and handling of Personal Data.

2.3.6 The Data Processor agrees to assist the Data Controller promptly with all subject information requests, rectification requests, erasure requests, requests for restriction of processing, objections or complaints which may be received from the data subjects of the Personal Data.

2.3.7 The Data Processor will notify and cooperate with the Data Controller promptly with requests made under the Freedom of Information Act 2000.

2.3.8 The Data Processor will not disclose the Personal Data to a third party in any circumstances other than at the specific written request of the Data Controller, unless the disclosure is required by law.

2.3.9 The Data Processor will transfer or store the Personal data only as permitted in Schedule B.

2.3.10 The Data Processor will not sub-contract any of the processing without explicit written agreement from the Data Controller, detailed in Schedule B. Where such written agreement is provided, the Data Processor will ensure that any sub-contractor it uses to process the personal data complies with the terms of this agreement.

2.3.11 The Data Processor will employ appropriate operational and technological processes and procedures summarised in Schedule E to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to be appropriate to the services being provided to the Data Controller.

2.3.12 The Data Processor will notify the Data Controller of any information security incident that may impact the processing of the personal data covered by this agreement within 2 working days of discovering, or becoming aware of any such incident. Following the report of the incident, the Data Processor will cooperate with the Data Controller's Compliance and Information Security staff whilst they carry out a risk assessment, root cause analysis and identify any corrective action required. The Data Processor will cooperate with the Data Controller in implementing any required corrective action agreed between the parties.

2.3.13 On satisfactory completion of the service or on termination of this agreement, the Data Processor will ensure that the personal data is securely removed from their systems and any printed copies securely destroyed. In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate methods.

2.3.14 The Data Controller reserves the right upon giving reasonable notice and within normal business hours to carry out compliance and information security audits of the data processor in order to satisfy itself that the Data Processor is adhering to the terms of this agreement. Where a sub-contractor is used, the Data Processor agrees that the Data Controller may also, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks of the sub-contractor to ensure adherence to the terms of this agreement.

2.4 THIRD PARTY RIGHTS

The Data Subject is hereby entitled to enforce the terms and conditions of this Agreement as a third party beneficiary.

2.5 LIABILITY

The Data Processor's liability to the Data Controller for any loss or damage of whatsoever nature suffered or incurred by the Data Controller or for any liability of the Data Controller to any other person for any loss or damage of whatsoever nature suffered or incurred by that person shall to the extent permitted by law not exceed the value shown in the Master Contract.

2.6 GOVERNING LAW

This Agreement shall be governed by and construed in accordance with English law and each party hereby submits to the non-exclusive jurisdiction of the English courts.

IN WITNESS WHEREOF, each of the Parties hereto has caused the Agreement to be executed by its duly authorised representative.

Signed for and on behalf of [Client Name]

Name	
Position	
Signature	
Date	

Signed for and on behalf of Sitekit Limited

Name	
Position	
Signature	
Date	

3 CMS system overview

This overview is for informational purposes only and does not form part of the agreement.

3.1 Background

The Sitekit CMS is a hosted or cloud-based content management system by which site administrators can create and edit their own websites.

The Sitekit CMS consists of web server(s) connected to a SQL database. The database can be provided as a hosted database and on-premise database or on a cloud based SQL instance in Azure.

Responsibility	Responsible organisation	Description
CMS administration system	Sitekit	Sitekit is responsible for the CMS administration system and its constituent parts that enables the administrator to create and edit web pages and store data.
CMS database	Sitekit	For hosted and cloud solutions Sitekit are responsible for the maintenance and running of the database server. Sitekit are not responsible for the content held in that database, just the database structure
CMS web server	Sitekit	For hosted and cloud solutions Sitekit are responsible for the maintenance and running of the web server
Content of web site	Data Controllers	The Data Controllers provide or commission the web site content consisting of but not limited to web pages, images, files and website visitor generated content.

Figure 1 - Key roles and responsibilities

4 Schedule A: Data transferred to the Data Processor

The Data Controller alone determines the data to be processed. The Data Processor shall receive and process data provided by the Data Controller under the following conditions. Data placed in a CMS system by the Controller which does not observe these conditions shall be at the Controller's sole risk.

Data classification	Conditions of processing	Notes
Unrestricted (public information)	Access to the administrative functions of the CMS system shall be restricted and credentials appropriately protected.	Unrestricted data can be processed with any CMS feature • Asset classes can be used to restrict the level of access that administrators have to areas of the site. • Password polices can be set on those admin credentials
Personal Information (e.g. names, emails, addresses)	Same conditions as the processing of Unrestricted information, plus: A GDPR compliant privacy notice must be published on the site; Users must consent to data sharing and processing, and must be able to withdraw consent; Data must be encrypted in transit via the https protocol; Access to data must be protected by appropriately configured access rights; Users must be able to contact the Data Controller to exercise their privacy rights.	Same facilities as the processing of unrestricted information as well as the following: • Sites can be created that run under the https protocol • Privacy notices can be created as normal CMS pages • Consent to data sharing can be edited into existing forms including subscription forms • Subscribers can be removed via the admin panel • Forms can be created in the CMS allowing web visitor to contact the relevant data controller's staff • Asset classes can be used to restrict site access on a least privilege principle
Sensitive information (GDPR's "Special Categories", e.g. health data)	Same conditions as the processing of Personal Information, plus: Relevant members of the Controller's staff must have completed CMS security training with Sitekit; Secure forms must be used; Data must be encrypted in transit via the https protocol and also whilst in storage.	Same facilities as the processing of personal information as well as the following: • Secure forms can be set up that encrypt any form submission when stored in the CMS database

Figure 2 - Dataset classifications and conditions of processing

5 Schedule B: Sub-processing and storage locations

The Data Controller permits the Data Processor to appoint the following sub-processors for the purposes of delivering CMS services:

- Microsoft Cloud Services (if applicable to your hosting plan)

The Data Controller permits the Data Processor to store the data described in Schedule A in the following locations:

- The Bunker (UK)
- Microsoft Azure (if applicable to your hosting plan)

6 Schedule C: Processing Purposes

Subject to a legal basis for processing, the Data Controller permits the Data Processor to process the data described in Schedule A for the following purposes only:

- Providing storage, retrieval, hosting and presentation services
- Providing support services to the Data Controller
- Improving and maintaining the above services

7 Schedule D: Legal basis for processing

Data will be processed in accordance with the Data Protection Act, NHS Information Governance standards and Regulation (EU) 2016/679 (GDPR) when incorporated into UK law.

The legal basis for processing of data by the Data Controller is the sole responsibility of the Controller, and may include any of the allowable legal bases. The Data Controller is responsible for establishing these bases and obtaining consent where necessary.

The legal bases for the processing by the Data Processor are:

- A commercial contract between the Controller and Processor for the supply, customisation, hosting and maintenance of a CMS solution (GDPR 6.1(a)); and
- Any legal obligation to which the Data Processor is subject, such as an instruction given by an authority (GDPR 6.1(b))

8 Schedule E: Security Measures

The Data Processor shall use its best endeavours to safeguard the Data from unauthorised or unlawful processing or accidental loss, destruction or damage and implement the measures outlined below to prevent unauthorised or unlawful processing or accidental loss or destruction of the Data:

8.1 Data Processor Information Governance Compliance

The Data Processor has maintained the NHS Digital IG Toolkit assessments since version 9 (2011/12) and is currently assessed at level 2 with a score of 76%, which is appropriate for a third party data processing organisation with N3 access. The Data Processor's ID is 8HT91 and the assessments can be viewed on the NHS Digital web site at:

https://www.igt.hscic.gov.uk/AssessmentReportCriteria.aspx?tk=426614283369262&lnv=3&cb=194c53ce-c8de-4065-80c1-11952ec26213&sViewOrgId=41798&sDesc=8HT91

The Data Processor also operates an Information Security Management System (ISMS) aligned with ISO 27001:2013.

8.2 Data Processor Quality Management compliance

The Data Processor is ISO 9001:2008 certified and is aiming at migration to ISO 9001:2015 by 2018.

8.3 Caldicott Guardian

The Data Processor has an appointed Caldicott Guardian and as part of the ISO 27001 processes. Relevant personnel with access to confidential data are trained in recognising and appropriately handling confidential and sensitive information. The training is based on NHS Digital materials.

8.4 Data Protection Act

All companies within the Data Processor's group are registered with the Information Commissioner's Office as Data Controllers in respect of their own business data, and have Data Processing Agreements with other clients in respect of data controlled by others. Annual reviews of overseas data transfer and storage locations are carried out. ICO registration details are at:

- Sitekit Ltd (Z8678329)
- Sitekit Applications Limited (ZA271976)
- Sitekit Health Limited (ZA272182)
- Sitekit Solutions Limited (ZA272192)
- Sitekit Systems Limited (ZA272173)

8.5 GDPR

The Data Processor has appointed a Data Protection Officer in compliance with GDPR legislation, due to come into effect from May 2018.

8.6 Microsoft SSPA programme

The Data Processor complies with the Microsoft Supplier Security and Privacy Assurance Programme.

8.7 Staff vetting

The Data Processor also complies with NHS Employment Checks. Disclosure and Barring Service checks are mandatory for new staff and are completed for existing staff. HMG's Baseline Personnel Security Standard checks are mandatory for staff working on Identity projects.

8.8 Access Control

The Data Processor has defined and operates an Access Control Policy in adherence to the requirements of ISO 27001:2013. Access is defined by individual and not by group.

8.9 Security Incidents

The Data Processor has defined and operates a Security Incident Management Procedure compliant with ISO 27001:2013 and the IG Toolkit which includes the analysis, resolution and notification of incidents affecting data security, integrity or availability..

8.10 Data Destruction

The Data Processor has defined and operates a Secure Data Deletion policy, which mandates the physical destruction of media that is no longer required, or the putting beyond use of data on media that will be re-used. In the case of data stored in cloud services, the Information Commissioner's Office accepts certain safeguards for putting beyond use data that maintains compliance with the Data Protection Act.

8.11 Microsoft Azure service security attributes

Some CMS instances are hosted on Microsoft Azure. The Data Processor confirms the following additional Microsoft Azure service security attributes:

8.11.1 ISO 27001 certification: Microsoft data centres are ISO 27001 certified and carry G-Cloud Impact Level 2 Accreditation from the Cabinet Office for use across the UK Public Sector.

8.11.2 Update management: Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application and database scans of the Azure environment.

8.11.3 Antivirus and antimalware: Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure virtual machines.

8.11.4 Penetration testing: Microsoft conducts regular penetration testing to improve Azure security controls and processes.

8.11.5 DDoS Protection: Azure has a defence system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defence system is designed to withstand attacks generated from outside and inside the platform.

8.12 Hosting security attributes

8.12.1 CMS is hosted by an ISO 27001 certified supplier.

8.12.2 CMS is hosted by a supplier compliant with NHS IGSoC.

8.12.3 CMS hosting is in an armoured, nuclear-bomb-proof and military-specified facility on the UK mainland.

8.13 CMS security attributes

8.13.1 CMS endpoints are secured using password based login.

8.13.2 CMS Administration system data is transferred using HTTPS (TLS).

8.13.3 User passwords on the CMS are encrypted at rest.

8.13.4 *Secure* forms submissions are encrypted at rest.

8.13.5 Data is only messaged/shared with identities verified as an authorised customer representative.

8.13.6 Customer CMS websites are secured via https only if the customer has purchased and configured the correct security certificate.

8.13.7 Communication between users and the relevant customer websites are secured via https only if the customer has purchased and configure the correct security certificate.

9 Schedule F: Service Level Agreement

Sitekit Ltd, the company that has developed CMS, provides service and support to customers. The specification of the service level agreement, including notifications and the maintenance and updates of the software, are detailed in the relevant contract.

9.1 Support

Sitekit's normal operating hours are Monday to Friday 9am to 5pm with emergency out of hours support, where included in the SLA.

Role	Contact details	Availability
General support	help@sitekit.net 0845 299 0900	Normal office hours
Emergency support	emergency@sitekit.net	24 x 7
Project management	ian.stewart@sitekit.net	Normal office hours
Information Security Manager / Data Protection Officer	john.yau@sitekit.net	Normal office hours
Caldicott guardian	Chris.eckl@sitekit.net	Normal office hours

10 Appendix 1: Data Controller privacy responsibilities

This appendix **does not form part of this Data Sharing Agreement** and is provided for information only. It is not exhaustive and does not constitute legal advice. Refer to the Data Protection Act 1998, Regulation (EU) 2016/679 ("GDPR") or a professional advisor for definitive information.

As a Data Controller, you should do the following:

- Carry out a Privacy Impact Assessment for your project if you are working with data classified as confidential and sensitive, e.g. health information any information that could be used to discriminate. The Privacy Impact Assessment must identify privacy risks arising from the project and the actions to mitigate them.
- You may need to appoint a Data Protection Officer if processing data in special categories in high volume.
- If you are acting as a joint Data Controller with other organisations, remember that users (Data Subjects) can exercise their rights with any of the joint Data Controllers. You should establish appropriate Data Sharing Agreements with other Controllers and a point of contact for Data Subjects.
- If you are processing data about individuals, you must publish a Privacy Statement that gives the user your contact details, a summary of the information collected and how it will be used.
- You must establish the legal basis for storing and processing data about individuals. A legal basis may be a contract, a legitimate business interest or the freely given consent of the Data Subjects. The legal basis for processing must be summarised in your Privacy Statement.
- If you use Consent as a legal basis for processing, consent must be freely given, must be obtained by positive action (not implied by omission) and presented in a manner clearly distinguishable from other matters in an intelligible and easily accessible form. Consent must be as easy to withdraw as it is to give.
- The granting and revocation of consent must be recorded.
- You must also provide mechanisms to allow individuals to object to processing, to change their details, to obtain a copy of their details, to withdraw consent for automated processing (profiling), to make a complaint, to request deletion of their data, or to request the sources of data that you hold. This can be as simple as giving people contact details to request changes. It does not necessarily need to be automated unless you anticipate a high volume of requests.
- If a data breach occurs, you may be required to notify data subjects in some circumstances.