

Lot 3 - Cloud Support Services (Additional Services)

SUPPLIER TERMS

The Supplier Terms (if any) applicable to this Call-Off Contract are as listed below.

Supplier Standard Terms

1. The Supplier Acceptable Use Policy listed below:

Not Applicable

2. The Supplier Data Processing Agreement listed below:

Data Processing Agreement attached

3. The Supplier Specific Shared Responsibility Model listed below:

Not Applicable

SUPPLIER SERVICE SPECIFIC TERMS

1. The Supplier SLA listed below:

Not Applicable

2. The Supplier Licence Terms listed below:

a. In these Supplier Licence Terms,

- i. **Authorised User** means a user permitted to access and use the Services
- ii. **Feedback** means any idea, suggestion, recommendation or request by you or any of your Personnel or Authorised Users or your customers, whether made verbally, in writing, directly or indirectly, in connection with the Services
- iii. **Intellectual Property Rights or Intellectual Property** means any and all existing and future rights throughout the world conferred by statute, common law, equity or any corresponding law in relation to any copyright, designs, patents or trade marks, business names, domain names, know-how, inventions, processes, trade secrets or confidential information, circuit layouts, software, computer programs, databases or source codes, including any application, or right to apply, for registration of, and any improvements, enhancements or modifications of, the foregoing, whether or not registered or registrable.
- iv. **Our Materials** means all Intellectual Property which is owned by or licensed to us (independent of this Call-Off Contract) and any improvements, modifications or enhancements of such Intellectual Property.
- v. **New Materials** means all Intellectual Property developed, adapted, modified or created by us for you under the Services, but excludes Our Materials and Your Materials
- vi. **Personnel** means, in respect of a Party, any of its employees, consultants, suppliers, subcontractors or agents, but in respect of you, does not include us

- vii. **Your Data** means the information, materials, logos, documents, qualifications and other Intellectual Property or data inputted by you, your Personnel and Authorised Users into the Services or stored by or generated by your use of the Services, including any Personal Information collected, used, disclosed, stored or otherwise handled in connection with this Call-Off Contract. Your Data does not include the Analytics, or any data or information that is generated as a result of your usage of the Services that is a back-end or internal output or an output otherwise generally not available to users of the Services
 - viii. **Your Materials** means all Intellectual Property owned or licensed by you or your Personnel before the date of this Call-Off Contract (which is not connected to this Call-Off Contract) and/or developed by or on behalf of you or your Personnel independently of this Call-Off Contract.
 - ix. **Services** means the Cloud Support Services the subject of this Call-Off Contract
 - x. **System** means all hardware, software, networks, telecommunications and other IT systems used by a Party from time to time, including a network
 - xi. **You or your** means the Buyer
 - xii. **Us, our or we** means the Supplier
- b. In connection with any of the Services, you agree:
- i. to provide all assistance, information, documentation, access, facilities and other things reasonably necessary to enable us to comply with our obligations under this Call-Off Contract;
 - ii. to provide us and our Personnel with reasonable, convenient and safe access to your premises and Systems to the extent reasonably necessary in order for us to supply the Services, and at the times agreed between the Parties;
 - iii. to ensure that any Systems used in connection with the Services have all necessary approvals and comply with all applicable laws;
 - iv. the Services are provided to you and your Authorised Users, solely for your (and your Authorised Users') benefit and you will not (or you will not attempt to) disclose, or provide access to, our Services to third parties without our prior written consent;
 - v. you will be responsible for the use of any part of the Services by your Authorised Users and any other person you provide with access to the Services, and you must ensure that no person uses any part of the Services:
 - 1. to break any law or infringe any person's rights (including Intellectual Property Rights);
 - 2. to transmit, publish or communicate material that is defamatory, offensive, abusive, indecent, menacing or unwanted; or
 - 3. in any way that damages, interferes with or interrupts the supply of the Services; and
 - 4. you will not alter or modify the Services in any way that is not contemplated by the purposes of the Services.
- c. As between the Parties, you acknowledge and agree that we own all Intellectual Property Rights in Our Materials and any Feedback, and you own all Intellectual Property Rights in Your Materials. As between the Parties, these Intellectual Property Rights will at all times vest, or remain vested, in us, and nothing in this Call-Off Contract constitutes an assignment or transfer of such Intellectual Property Rights. To the extent that ownership of these Intellectual Property Rights does not automatically vest in us, you hereby assign all such Intellectual Property Rights to us and agree to do all other things necessary to assure our title to such rights.
- d. You agree that:
- i. we may use Feedback in any manner which we see fit (including to develop new features) and no benefit will be due to you as a result of any use by us of any Feedback;
 - ii. you must not whether directly or indirectly, without our prior written consent:
 - iii. take any action that may compromise or jeopardise our Intellectual Property Rights in the Services or otherwise; or
 - iv. remove or deface any confidentiality, copyright or other proprietary notice placed on the Services.
- e. As between the Parties, you will continue to own all Intellectual Property Rights in Your Materials and New Materials.

- f. You grant us a non-exclusive, revocable, worldwide, non-sublicensable (other than to companies within our 'group', as that term is defined in the Companies Act 2006) and non-transferable right and licence, to use Your Materials and the New Materials, solely for the performance of our obligations or exercising our rights under this Call-Off Contract.
- g. As between the Parties:
 - i. Your Data is and will remain your property; and
 - ii. you retain any and all rights, title and interest in and to Your Data, including all copies, modifications, extensions and derivative works.
- h. You grant us a limited licence to copy, transmit, store, backup and/or otherwise access or use Your Data during the Term (and for a reasonable period after the Term), to:
 - i. supply the Services to you (including to enable you and your Personnel to access and use the Services), and otherwise perform our obligations under this Call-Off Contract;
 - ii. diagnose problems with the Services;
 - iii. enhance and otherwise modify the Services;
 - iv. perform Analytics;
 - v. develop other services, provided we de-identify Your Data; and
 - vi. as reasonably required to perform our obligations under this Call-Off Contract.
- i. You acknowledge and agree that:
 - i. we are not responsible for the integrity or existence of any data on any System, network or any device controlled by you, your Authorised Users or your Personnel; and
 - ii. we assume no responsibility or liability for Your Data. You are solely responsible for Your Data and the consequences of using, disclosing, storing or transmitting it. It is your responsibility to backup Your Data.
- j. You represent, warrant, acknowledge and agree that:
 - i. you have obtained all necessary rights, releases and permissions to provide or have Your Data provided to us and to grant the rights granted to us in this Call-Off Contract;
 - ii. Your Data (and its transfer to and/or use, collection, storage or disclosure by us as contemplated by this Call-Off Contract) does not and will not violate any laws (including those relating to export control and electronic communications) or the rights of any third party, including any Intellectual Property Rights, rights of privacy, or rights of publicity; and
 - iii. the operation of the Services is reliant on the accuracy and completeness of Your Data, and the provision by you of Your Data that is inaccurate or incomplete may affect the use, output and operation of the Services.
- k. You acknowledge and agree that we may monitor, analyse and compile statistical and performance information based on and/or related to your use of the Services, in an aggregated and anonymised format (Analytics). You agree that we may make such Analytics publicly available, provided that it:
 - i. does not contain any identifying information; and
 - ii. is not compiled using a sample size small enough to make underlying portions of Your Data identifiable.
- l. We, and our licensors own all right, title and interest in and to the Analytics and all related software, technology, documentation and content used or provided in connection with the Analytics, including all Intellectual Property Rights in the foregoing.
- m. We may use and disclose to our service providers anonymous data about your access and use of the SaaS Solution for the purpose of helping us improve the SaaS Solution. Any such disclosure will not include details of your, or any Authorised User's, identity or personal information.

DATA PROCESSING ADDENDUM

This Data Processing Addendum (**DPA**) supplements the terms of the Call-Off Contract that this DPA is attached to (in particular being under the 'Supplier Terms') (**Agreement**) and applies to our provision of Services to you under the Agreement (as the Parties are defined in the Agreement). This DPA applies from the date you agree to our Agreement, and will continue in accordance with the terms of this DPA.

1. Definitions

1.1 Capitalised terms in this DPA have the meaning given in the Agreement, the Annexures, and as set out below:

EU GDPR means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

Transferred Data means any Personal Data Processed by us or our Personnel on behalf of you in connection with the Agreement.

Restricted Transfer means a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

UK GDPR means the EU GDPR as incorporated into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

UK Addendum means the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers approved by the Information Commissioner's Office under section 119A of the Data Protection Act 2018 on 21 March 2022 (version B.1.0), and as updated from time to time.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processor", "Processing" and "Sub-Processor" shall have the same meaning as in the UK GDPR.

2. Roles of the Parties

The Parties acknowledge and agree that in connection with the Agreement, where you provide us with Transferred Data, we are the Processor and you are the Controller.

3. Processing of Personal Data

3.1 Each Party agrees to comply with Applicable Data Protection Law in the Processing of Transferred Data.

3.2 You instruct us to process Transferred Data in accordance with this DPA (including in accordance with Annex 1).

3.3 We agree to not process Transferred Data other than on your documented instructions.

4. Our Personnel

We agree to take reasonable steps to ensure the reliability of any of our Personnel who may have access to the Transferred Data, ensuring in each case that:

- (a) access is strictly limited to those individuals who need to know / access the relevant Transferred Data, as strictly necessary for the purposes of the Agreement; and
- (b) the relevant Personnel are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we agree to implement appropriate technical and organisational measures in relation to the Transferred Data to

ensure a level of security appropriate to that risk in accordance with Applicable Data Protection Law, and as further particularised in Annex 2.

- 5.2 In assessing the appropriate level of security, we agree to take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Sub-Processing

- 6.1 You authorise our engagement of the Sub-Processors already engaged by us at the date of this DPA, which are set out at Annex 3.

- 6.2 Where we wish to engage a new Sub-Processor, we agree to provide written notice to you of the details of the engagement of the Sub-Processor at least 14 days' prior to engaging the new Sub-Processor (including details of the processing it will perform). You may object in writing to our appointment of a new Sub-Processor within 7 days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the Parties will discuss such concerns in good faith with a view to achieving resolution. If the Parties are not able to achieve resolution, we may, at our election:

- (a) not appoint the proposed Sub-Processor;
- (b) not disclose any Transferred Data we process on your behalf to the proposed Sub-Processor; or
- (c) inform you that we may terminate the Agreement (including this DPA) for convenience, in which case, clause **Error! Reference source not found.** will apply.

- 6.3 You agree that the remedies described above in clauses 6.2(a) to 6.2(c) are the only remedies available to you if you object to our engagement of any proposed Sub-Processor by us.

- 6.4 Where we engage a Sub-Processor to process Transferred Data, we agree to enter into a written agreement with the Sub-Processor containing data protection obligations no less protective than those in this DPA with respect to the Transferred Data, and to remain responsible to you for the performance of such Sub-Processor's data protection obligations under such terms.

- 6.5 Where the transfer of Transferred Data from us to a Sub-Processor is a Restricted Transfer, it will be subject to the UK Addendum (and documents or legislation referred to within it), which shall be deemed to be incorporated into this DPA, and the UK Addendum is considered an appropriate safeguard.

7. Data Subject Rights

- 7.1 Taking into account the nature of the Processing, we agree to assist you by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of your obligations, as reasonably understood by you, to respond to requests to exercise Data Subject rights under the Applicable Data Protection Law.

- 7.2 We agree to:

- (a) promptly notify you if we receive a request from a Data Subject under any Applicable Data Protection Law in respect of Transferred Data; and
- (b) ensure that we do not respond to that request except on your documented instructions or as required by Applicable Data Protection Law to which we are subject, in which case we shall, to the extent permitted by Applicable Data Protection Law, inform you of that legal requirement before we (or our Sub-Processor) respond to the request.

8. Personal Data Breach

- 8.1 We agree to notify you without undue delay upon becoming aware of a Personal Data Breach affecting Transferred Data, and to provide you with sufficient information to allow you to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

- 8.2 We agree to co-operate with you and take reasonable commercial steps as directed by you to assist in the investigation, mitigation and remediation of each such Personal Data Breach.
- 8.3 If you decide to notify a Supervisory Authority, Data Subjects or the public of a Personal Data Breach, you agree to provide us with advance copies of the proposed notices and, subject to Applicable Data Protection Law (including any mandated deadlines under the UK GDPR), allow us an opportunity to provide any clarifications or corrections to those notices.

9. Data Protection Impact Assessment and Prior Consultation

We agree to provide reasonable assistance to you with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which you reasonably consider to be required by article 35 or 36 of the UK GDPR or equivalent provisions of any other Data Protection Law (to the extent you do not otherwise have access to the relevant information and such information is in our control).

10. Deletion or return of Personal Data

Subject to this clause 11, and subject to any document retention requirements at law, we agree to promptly and in any event within 30 business days of the date of cessation of any Services involving the Processing of Transferred Data (**Cessation Date**), delete and procure the deletion of all copies of those Transferred Data.

11. Audit Rights

- 11.1 Subject to this clause 11, where required by law, we shall make available to you on request all information reasonably necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by you or an auditor mandated by you in relation to the Processing of Transferred Personal Data by us.
- 11.2 Where clause 11.1 applies, any audit (or inspection):
- (a) must be conducted during our regular business hours, with reasonable advance notice (which shall not be less than 30 business days);
 - (b) will be subject to our reasonable confidentiality procedures;
 - (c) must be limited in scope to matters specific to you and agreed in advance with us;
 - (d) must not require us to disclose to you any information that could cause us to breach any of our obligations under Applicable Data Protection Law;
 - (e) to the extent we need to expend time to assist you with the audit (or inspection), this will be funded by you, in accordance with pre-agreed rates; and
 - (f) may only be requested by you a maximum of one time per year, except where required by a competent Supervisory Authority or where there has been a Personal Data Breach in relation to Transferred Personal Data, caused by us.
- 11.3 Your information and audit rights only arise under clause 11.1 to the extent that the Agreement does not otherwise give you information and audit rights that meet the relevant requirements of Applicable Data Protection Law.

12. Liability

Despite anything to the contrary in the Agreement or this DPA, to the maximum extent permitted by law, the Liability of each Party and its affiliates under this DPA is subject to the exclusions and limitations of Liability set out in the Agreement.

13. Termination

- 13.1 Each Party agrees that a failure or inability to comply with the terms of this DPA and/or the Applicable Data Protection Law constitutes a material breach of the Agreement. In such event, you may, without penalty:
- (a) require us to suspend the processing of Transferred Data until such compliance is restored; or
 - (b) terminate the Agreement effective immediately on written notice to us.
- 13.2 In the case of such suspension or termination by you, we shall provide a prompt pro-rata refund of all sums paid in advance under the Agreement which relate to the period of suspension or the period after the date of termination (as applicable).
- 13.3 Notwithstanding the expiry or termination of this DPA, this DPA will remain in effect until, and will terminate automatically upon, deletion by us of all Transferred Data covered by this DPA, in accordance with this DPA.

ANNEX 1

DESCRIPTION OF TRANSFER

Personal Data Transferred	• Identity Data including first name, middle name, last name, maiden name, title, date of birth, gender, job title, marital status, and pronouns. • Contact Data including billing addresses, delivery addresses, email addresses and telephone numbers. • Employee details including Identity Data and Contact Data of past, present and future employees. • Financial Data including bank account and payment card details.
Special Categories of Personal Data and criminal convictions and offences	The transferred data includes data relating to: • racial or ethnic origin • religious or philosophical beliefs • genetic data • physical or mental health • sex life or sexual orientation
Relevant Data Subjects	• your patients and clients • your employees, contractors and other personnel • any third parties involved in the care of your patients and clients • anyone about whom personal data is input into the Services
Frequency of the transfer	Continuous
Nature of the transfer	As specified in the Agreement, and this DPA, including without limitation: • use of Transferred Data to provide the Services; • collection, organisation, storage (hosting), retrieval and other processing of Transferred Data necessary to provide, maintain and improve the Services; and • as compelled by law.
Purpose of processing	The purpose of the transfer and processing are as specified in the Agreement and this DPA.
Duration of the Processing	The term of the Agreement and for a period of 30 days after termination or expiry of the Agreement.

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

TECHNICAL AND ORGANISATIONAL MEASURES	DETAILS
Designated data protection officer (if required) or privacy manager	Roger de la Fuente Garcia
Security certifications	• DSPT • Cyber Essentials • ICO registration
Internal policies e.g. security policy, data retention and deletion policies	• We maintain a data registry detailing all data retention policies for different types of data, including resident and worker data, which can be provided on request.
Pseudonymisation and encryption of personal data	• All client generated information (including all personal data and its relevant backup copies) is encrypted using a dedicated encryption key stored in Amazon AWS KMS
Product security features	• Single sign on is supported through the client's Microsoft Azure AD, with optional multi-factor features available. Audit logs of the identity features are available.
Network security	• Amazon AWS is our sole network provider, and links to their relevant compliance policies can be found here: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html • Production environments of the product are provided with complete physical isolation from public networks through AWS VPC networks, and all change activities are audited through associated Control Tower policies. •
Physical security and disaster recovery	• We don't operate physical locations directly, and rely on physical security and access controls implemented by Amazon AWS and our other network providers. • More information about AWS physical security measures can be found here:

	https://aws.amazon.com/trust-center/data-center/our-controls/
Human resources security	• Appropriate background checks are conducted on all employees in accordance with documented policies. • Business obtains written commitment of employees and contractors to maintain confidentiality in employment contracts and contractors agreements. • Access is revoked on a timely basis in accordance with security procedures upon the departure of any personnel. • Password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords. • Deliver regular (at least annually) information security awareness training to all employees.
Insert any further technical and organisation security measures in place	Our change management practices include PRGB controls on all code changes, with manual approval before production

ANNEX 3

LIST OF SUBPROCESSORS

SUB-PROCESSOR	LOCATION	PURPOSE/ SERVICES	WEBSITE & CONTACT DETAILS
Amazon Web Services EMEA SARL	London / United Kingdom data center (eu-west-2)	Cloud services	https://aws.amazon.com 38 Avenue John F. Kennedy, Luxembourg 1855, Luxembourg
Auth0 Ltd	United Kingdom data center	User authentication	https://auth0.com/contact-us 20 Farringdon Rd, London EC1M 3HE
MessageBird UK Ltd (Pusher Ltd)	EU data center	Client – server message broker	https://pusher.com/ 4 th Floor, 3 More London Riverside, London SE1 2AQ
Microsoft Corporation (Azure)	London / United Kingdom data center (UK south)	Cloud services (off-site backup data copies)	https://azure.microsoft.com One Microsoft Way, Redmond, WA 98052, USA