Lot 2B – Software as a Service (Saas)

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:

a. In this Supplier Acceptable Use Policy:
   i. **Account** means an account accessible to the Buyer and/or Authorised Users to use the Services, including the SaaS Solution.
   ii. Authorised User means a user permitted to access and use the Services under the Buyer's Account.
   iii. **Buyer** means the Buyer and its Authorised Users
   iv. **Harmful Code** means any computer program or virus or other code that is harmful, destructive, disabling or which assists in or enables theft, alternation, denial of service, unauthorised access to or disclosure, destruction or corruption of information or data.
   v. **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.
   vi. **Personnel** means, in respect of a Party, any of its employees, consultants, suppliers, subcontractors or agents, but in respect of the Buyer, does not include the Supplier.
   vii. **SaaS Licence** means the licence granted by the Supplier to the Buyer for access to and use of the SaaS Solution, in accordance with the 'Supplier Licence Terms'
   viii. **SaaS Solution** means the cloud-based software solution provided under this Call-Off Contract.
   ix. **Services** means the software-as-a-service services provided by the Supplier under 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 and any Authorised Users.

   1.1.1 **We**, **us** or **our** means the Supplier.

b. You must not (and you must ensure that each Authorised user does not):
   i. access or use the SaaS Solution except as permitted by the SaaS Licence, or other than through the interface we provide;
   ii. access or use the SaaS Solution in any way that is improper or breaches any applicable laws, infringes any person's rights (including Intellectual Property Rights and privacy rights), or gives rise to any civil or criminal liability;
   iii. interfere with or interrupt the supply of the SaaS Solution or our System, or any other person's access to or use of the SaaS Solution;
   iv. introduce any Harmful Code into the SaaS Solution or our System;
   v. directly or indirectly use, copy, decompile or reverse engineer the SaaS Solution;
   vi. allow others to access or use your Account (or in the case of Authorised Users, their login details), including any password or authentication details;
   vii. rent or sublicence the use of the Services to any third parties, without our prior written consent or as otherwise permitted under this Call-Off Contract;
   viii. use the SaaS Solution to carry out security breaches or disruptions of a network;
   ix. attempt to access any data or log into any server or account that you are not expressly authorised to access;
   x. circumvent user authentication or security of any of our networks, accounts or hosts or those of any third party; or

xi. access or use the SaaS Solution to transmit, publish or communicate material that is, defamatory, offensive, abusive, indecent, menacing, harassing or unwanted.

c. 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 or at law;
   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 all information provided to us is kept up-to-date and the email address you provide is valid and regularly checked;
   iv. to ensure that any Systems used in connection with the Services have all necessary approvals and comply with all applicable laws;
   v. that you are responsible for all Authorised Users and other users within your organisation or within your control using the Services, including your Personnel.
d. You acknowledge and agree that:
   i. 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;
   ii. 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:
   iii. to break any Law or infringe any person's rights (including Intellectual Property Rights);
   iv. to transmit, publish or communicate material that is defamatory, offensive, abusive, indecent, menacing or unwanted; or
   v. in any way that damages, interferes with or interrupts the supply of the Services; and
   vi. you will not alter or modify the Services in any way that is not contemplated by the purposes of the Services.
e. You must ensure that any information provided to us for any Account or login is accurate and complete, and you warrant that you are authorised to provide this information to us.
f. You and your Authorised Users must keep your Account and login details secure and confidential. You agree to immediately notify us if you become aware of, or have reason to suspect, any suspicious or unauthorised access to your Account or use of any login details linked to your Account.
g. You will ensure each Authorised User complies with the terms of this Call-Off Contract.

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

2. The Supplier SLA listed below:

This Service Level Agreement (**SLA**) applies to the Services provided under this Call-Off Contract

1. Definitions

Unless the context requires otherwise, the following definitions apply in this SLA:

a. **Account** has the meaning in the Supplier Acceptable Use Policy.
b. **Acknowledgement** means the Supplier's acknowledgement of the Buyer's notification of an Incident or, where the Supplier becomes aware of an Incident, the Supplier's notice of the Incident to the Buyer.
c. **Authorised User** means a user permitted to access and use the Services under the Buyer's Account.
d. **Availability** means $\frac{\textit{Total Minutes} - \textit{Downtime}}{\textit{Total Minutes}} \times 100$
e. **Availability Target** means 99.5%.
f. **Buyer** has the meaning in the Supplier Acceptable Use Policy.
g. **Downtime** means the number of whole minutes within the relevant calendar month that the Buyer is unable to access the SaaS Solution. Downtime does not include the time that the SaaS Solution is unavailable due to Scheduled Downtime, Emergency Maintenance or an Excluded Event.
h. **Emergency Maintenance** means any maintenance deemed necessary to protect and maintain the security or integrity of the SaaS Solution.
i. **Excluded Event** means each of the following:
    i. failure caused by any software, hardware or other components outside the Supplier's network or not provided by the Supplier;
    ii. any trial or beta software (being any software released to the market for testing and feedback);
    iii. Force Majeure Event;
    iv. any resource reduction directed and approved in writing by the Buyer despite the Supplier's written notice that such reduction may result in that failure or less than optimum performance;
    v. any modification, revision, variation, translation or alteration of the SaaS Solution that is not authorised by the Supplier;
    vi. failure of access circuits to the Supplier's network or upstream providers, unless such failure is caused solely by the Supplier;
    vii. the Buyer's acts or omissions (or the acts or omissions of others engaged or authorised by the Buyer), including, without limitation, any negligence, wilful misconduct, or use of the SaaS Solution in breach of this Call-Off Contract;
    viii. outages elsewhere on the internet that hinder or prevent access to the SaaS Solution or the Buyer's Account;
    ix. failure caused by the Buyer's Data;
    x. failure caused by third party products or services; and
    xi. IP address blacklisting by third parties.
j. **Force Majeure Event** means any event or circumstance which is beyond a Party's reasonable control including but not limited to, acts of God, civil riot, terrorism, war, pandemic or epidemic.
k. **Incident** means defect, error, bug or malfunction in the Services that is not caused, or contributed to, by the Buyer.
l. **Response Time** means the time between the Buyer's proper notification of an Incident and the Supplier's Acknowledgement, or where the Supplier first becomes aware of an Incident, the time between the Supplier becoming aware of the Incident and the Supplier's Acknowledgement.
m. **Resolution Time** means the time between the Supplier's Acknowledgement and the time by which the Supplier removes or blocks a security threat, restores the Services to its specifications or finds a suitable workaround which restores the Services so as to allow the Buyer to continue using the Services without major interruptions or a major loss of functionality.
n. **Scheduled Downtime** means planned maintenance or upgrades to the SaaS Solution in accordance with this Call-Off Contract.
o. **Total Minutes** means the total number of minutes in the relevant calendar month.

2. Service Level – Availability

During the term of this Call-Off Contract, the Supplier will use commercially reasonable efforts to provide the Buyer with the SaaS Solution in accordance with the Availability Target.

3. Service Levels – Response Times

The Supplier will use commercially reasonable endeavours to provide the Target Services in response to Incidents in accordance with the following Service Levels:

SUPPORT PRIORITY	SERVICE AVAILABILITY	RESPONSE TIME	RESOLUTION TIME	STATUS UPDATES
1	24 hours per day, 7 days per week (including public holidays)	1 business hour	4 business hours	Hourly
2	24 hours per day, business days	4 business hours	8 business hours	Every 4 hours
3	9am-5pm, business days	1 business day	5 business days	Daily
4	9am-5pm, business days	2 business days	10 business days	Daily

4. Time measurement

a. The "Response Time", "Resolution Time" and "Status Update" obligations in the table above are subject to the "Service Availability" window.

b. If an Incident is notified to the Supplier outside the applicable Service Availability window, time measurement will begin from the commencement of the next Service Availability window for that priority classification for that Incident. For example, if a Priority 3 Incident is raised at 5:30pm on a Thursday and the Service Availability window for Priority 3 closed at 5:00pm, then the time measurement will not commence until the commencement of the next Service Availability window which would be 9am on the next Business Day.

5. After hours support

For Incidents that occur outside the Service Availability times (that is after hours), response and resolution times will only remain active (or extend beyond the Service Availability period) for Priority 1 Incidents. For all other Incidents raised after hours, response and resolution times will only become active upon the commencement of the next Service Availability period i.e. 9am. For Priority 2, 3 and 4 Incidents raised during the Service Availability period, the Supplier will not continue to work on the Incident, and the response and resolution times will be paused after hours. The Supplier will recommence work on the Incident, and the response and resolution times will continue from the commencement of the next Service Availability period.

6. Service Level Priority definitions

PRIORITY 1	PRIORITY 2	PRIORITY 3	PRIORITY 4
The service failure creates a serious business and financial exposure, or risk of harm to service users.	The service failure creates a significant business and financial exposure.	The service failure creates a low business and financial exposure.	The service failure creates a minimal business and financial exposure.

3. The Supplier Licence Terms listed below:

1. Definitions

In these Supplier Licence Terms the same definitions in the Supplier Acceptable Use Policy apply, and

a. **API** means a third party software application
b. **Licence** means these Supplier Licence Terms
c. **Third Party Inputs** means third parties or any goods and services provided by third parties, including customers, end users, suppliers, transportation or logistics providers or other subcontractors which the provision of the Services may be contingent on, or impacted by, including any API.
d. **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 data 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.

2. Licence

a. The terms of this Licence are in addition to and supplement the Supplier Acceptable Use Policy terms.
b. During the term of this Call-Off Contract, and subject to your compliance with this Call-Off Contract,, we grant you and each Authorised User a non-exclusive, non-transferable, non-sublicensable and revocable licence to access and use the SaaS Solution solely for your business purposes
c. Certain features of the SaaS Solution may be powered by API(s) supplied by third parties. Your use of such features may be subject to additional terms of service provided by the supplier of the relevant third party API.
d. When using the SaaS Solution, you must not do or attempt to do anything that is unlawful or inappropriate, including:
    1.1.1 anything that would constitute a breach of an individual's privacy (including uploading private or personal information without an individual's consent) or any other legal rights;
    1.1.2 using the SaaS Solution to defame, harass, threaten, menace or offend any person, including using the SaaS Solution to send unsolicited electronic messages;
    1.1.3 tampering with or modifying the SaaS Solution (including by transmitting viruses and using trojan horses);
    1.1.4 using data mining, robots, screen scraping or similar data gathering and extraction tools on the SaaS Solution; or
    1.1.5 facilitating or assisting a third party to do any of the above acts.
e. You acknowledge and agree that the SaaS Solution may be reliant on, or interface with third party systems that are not provided by us (for example, third party APIs, cloud storage providers, CRM systems, and internet providers) (Third Party Services). To the maximum extent permitted by law, we shall have no Liability for any Third Party Services, or any unavailability of the SaaS Solution due to a failure of the Third Party Services.
f. You acknowledge and agree that data loss is an unavoidable risk when using any software. To the extent you input any data into the SaaS Solution, you agree to maintain a backup copy of any data you input into the SaaS Solution.
g. Should we suspect that you are in breach of this Licence, we may suspend your access to the SaaS Solution while we investigate the suspected breach.
h. You represent, warrant and agree that:
    i. you will not use our SaaS Solution, including Our Intellectual Property, in any way that competes with our business;
    ii. you have not relied on any representations or warranties made by us in relation to the SaaS Solution (including as to whether the SaaS Solution is or will be fit or suitable for your particular purposes), unless expressly stipulated in this Call-off Contract.
i. The SaaS Solution may contain links to websites operated by third parties. Unless we tell you otherwise, we do not control, endorse or approve, and are not responsible for, the content on those websites. We recommend that you make your own investigations with respect to the suitability of those websites. If you purchase goods or services from a third party website linked from the SaaS Solution, such third party provides the goods and services to you, not us. We may receive a benefit (which may include a referral fee or a commission) should you visit certain third-party websites via a link on the SaaS Solution (**Affiliate Link**) or for featuring certain products or services on the SaaS Solution. We will make it clear by notice to you which (if any) products or services we receive a benefit to feature on the SaaS Solution, or which (if any) third party links are Affiliate Links

3. **Access to the SaaS Solution**
   a. You agree not to attempt to circumvent any relevant identity and access management controls or share your organisational credentials with any other person. Your authenticated session is personal to you and must not be transferred to others.
   b. You are responsible for maintaining the security of your organisational credentials in accordance with your organisation's security policies. While authentication is managed through your organisation's identity platform, you remain liable for all activity conducted through your authenticated sessions. You agree to immediately notify both us and your organisation's IT administrator of any suspected unauthorised use of your account or credentials.
4. **Our Intellectual Property**
   a. You acknowledge and agree that any Intellectual Property or content (including copyright and trademarks) available on the SaaS Solution, the SaaS Solution itself, and any algorithms or machine learning models used on the SaaS Solution (**Our Intellectual Property**) will at all times vest, or remain vested, in us.
   b. We authorise you to use Our Intellectual Property solely for your limited commercial use. You must not exploit Our Intellectual Property for any other purpose, nor allow, aid or facilitate such use by any third party.
   c. You must not, without our prior written consent:
      i. copy, in whole or in part, any of Our Intellectual Property;
      ii. reproduce, retransmit, distribute, disseminate, sell, publish, broadcast or circulate any of Our Intellectual Property to any third party; or
      iii. breach any intellectual property rights connected with the SaaS Solution, including (without limitation) altering or modifying any of Our Intellectual Property, causing any of Our Intellectual Property to be framed or embedded in another website, or creating derivative works from any of Our Intellectual Property.
5. **Third Party Inputs**
   a. You acknowledge and agree that the Services may interact with, or be reliant on, certain Third Party Inputs, including any API with, or be reliant on, certain Third Party Inputs,
   b. You acknowledge and agree that
      i. you are responsible for obtaining and managing all licences for the relevant Third Party Inputs;
      ii. you are responsible for paying all fees related to the Third Party Inputs; and
      iii. you agree to comply with terms and conditions applicable to the relevant Third Party Inputs at all times.
      iv. We do not make any warranty or representation in respect of any Third Party Inputs.
      v. To the maximum extent permitted by law, we will not be liable for, and you waive and release us from and against, any liability caused or contributed to by, arising from or connected with any Third Party Inputs.
6. **Your Data**
   a. 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.
   b. You grant us a limited licence to copy, transmit, store, backup and/or otherwise access or use Your Data during the term of this Call-off Contract (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.
   c. You acknowledge and agree that:
      i. we are not responsible for the integrity or existence of any data on your systems, 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.
   d. 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.

7. Analytics

a. 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.

b. 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.

c. 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 that 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/ 4th 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