Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the agreement between You and Crowd Connected Ltd ("**CC**") (the "**Agreement**") and sets out the terms on which CC processes Personal Data on Your behalf.

1. In this DPA, the following terms shall have the meanings set out below:

   "Alias" means a customer-provided identifier (such as an app install identifier, badge scan identifier, or other unique reference) that You transmit to CC, whether via the CC SDK, CC-published mobile applications, file transfer, or any other means, for the purpose of linking Device Identifiers to Your own records.

   "Anonymised Data" means Customer Data from which all Aliases have been removed and in respect of which You no longer retain any mapping capable of re-identifying a natural person from the remaining Device Identifiers and associated data.

   "AWS" means Amazon Web Services, Inc.

   "Customer Data" means all data that CC processes on Your behalf in connection with the Agreement, comprising Device Identifiers, location coordinates, place observations, device information, diagnostic data, and any Aliases You provide. Customer Data does not include occupancy counting data derived from hashed rotating device identifiers, which constitutes anonymous aggregate data not capable of identifying a natural person.

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

   "Data Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

   "Data Processor" means a natural or legal person which processes Personal Data on behalf of the Data Controller.

   "Device Identifier" means a random identifier generated by CC's software (such as an SDK instance identifier or tag identifier) that does not, in isolation, identify a natural person.

   "EEA" means the European Economic Area.

   "Personal Data" has the meaning given to it in applicable Data Protection Legislation.

   "Supplemental Agreement" has the meaning given to it in Clause 11 of this DPA.

2. You are the Data Controller and CC is a Data Processor in respect of Customer Data. CC shall process Customer Data only in accordance with Your documented instructions as set out in this DPA and the Agreement.

3. The Parties acknowledge that Customer Data constitutes pseudonymised Personal Data from Your perspective as Data Controller, because You hold (or are capable of creating) the means to re-identify natural persons from Device Identifiers – whether through Aliases transmitted to CC or through mappings You maintain independently. CC does not hold the means to identify any natural person from Customer Data without additional information held by You.

4. You shall ensure that any Alias provided to CC by You or Your contractors does not contain or comprise information that directly identifies a natural person (such as a name, email address, phone number, postal address, or government-issued identification number). Any Alias must not enable CC to identify a natural person without access to additional information held exclusively by You. Any Alias shall not include Special Categories of Personal Data (which would require enhanced safeguards consistent with Article 9 GDPR).

5. The processing carried out by CC under this DPA is further specified as follows:

Subject matter and duration of processing	Processing of Customer Data for the duration of the Agreement
Nature and purpose of processing	Collection and processing of indoor positioning data (comprising Device Identifiers, location coordinates,

	place observations, device information, and diagnostic data) and, where provided, Aliases, for the purpose of delivering location-based services including wayfinding, asset tracking, and spatial analytics, and for debugging and service improvement
Type of Personal Data	Pseudonymised location data comprising Device Identifiers, location coordinates, place observations, device information, diagnostic data, and Aliases (where provided)
Categories of Data Subjects	Attendees, visitors, delegates, patients, or other individuals whose devices interact with CC's positioning infrastructure, as determined by the Customer

6. You warrant that:

   (a) You have a lawful basis under applicable Data Protection Legislation for the processing of Customer Data by CC as described in this DPA, including any necessary consents, notices, or legitimate interest assessments;

   (b) You shall not instruct CC to process Customer Data in a manner that would cause CC to breach applicable Data Protection Legislation; and

   (c) You acknowledge that CC cannot identify any natural person from Customer Data without additional information held by You, and that the classification of Customer Data as Personal Data arises from Your ability (as Data Controller) to re-identify individuals.

7. CC warrants that it shall:

   (a) implement and maintain appropriate technical and organisational measures to protect Customer Data against unauthorised or unlawful processing and against accidental loss, destruction, or damage, having regard to the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing;

   (b) process Customer Data only on Your documented instruction, including transfers of Personal Data to third countries or international organisations, unless required to do so by applicable law, in which case CC shall inform You of that legal requirement before processing (unless prohibited from doing so). For the avoidance of doubt, Your execution of this Agreement constitutes a documented instruction to CC to transfer Customer Data in accordance with this DPA, and no further instruction shall be required in respect of that transfer for the duration of the Agreement;

   (c) not transfer Customer Data outside the UK or EEA except in accordance with Clause 7;

   (d) maintain records of all processing activities carried out on Your behalf, as required by Article 30(2) UK GDPR;

   (e) ensure that persons authorised to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that access to Customer Data is limited to those personnel who require it for the performance of the Agreement;

   (f) cooperate with and assist any supervisory authority in the performance of its tasks, where required by applicable Data Protection Legislation;

   (g) taking into account the nature of the processing and the information available to CC, assist You in ensuring compliance with Your obligations under Articles 32 to 36 UK GDPR (as applicable), including in relation to security of processing, data protection impact assessments, and prior consultation with supervisory authorities. CC shall not respond directly to any data subject request unless expressly instructed by You or required by law;

(h) at Your choice, delete or return all Customer Data to You within 90 days after the end of the provision of services relating to the processing, and delete existing copies unless applicable law requires storage of the Customer Data; and

(i) make available to You all information necessary to demonstrate compliance with the obligations laid down in Article 28 UK GDPR, and allow for and contribute to audits, including inspections, conducted by You or an auditor mandated by You, subject to reasonable prior notice and confidentiality arrangements.

8. CC is hereby authorised to engage the third-party sub-processors identified herein in connection with this DPA, provided always that (1) CC has entered into a written agreement with each sub-processor containing data protection obligations no less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the service provided by such sub-processor; (2) CC shall remain fully liable for the performance of each of its authorised sub-processors and (3) CC shall provide at least thirty (30) days' prior written notice of any intended addition or replacement of a sub-processor. CC shall provide at least thirty (30) days' prior written notice of any intended addition or replacement of a sub-processor. You may object on reasonable data protection grounds and, if unresolved, may terminate the affected services.

List of authorised sub-processors:

Name	**Purpose**	**Location**
AWS	Cloud computing services	USA or another jurisdiction providing an adequate level of protection for Personal Data pursuant to Clause 7 below

CC shall comply with any other applicable data protection regulations, whether in relation to UK GDPR, GDPR, or otherwise.

9. Where CC (or any sub-processor) transfers Customer Data outside the UK or EEA to a jurisdiction not subject to an adequacy decision applicable to the transfer, the Parties shall ensure that the transfer is subject to appropriate safeguards under Article 46 UK GDPR / GDPR (as applicable), such as the UK International Data Transfer Agreement or Addendum and/or the EU Standard Contractual Clauses, together with any supplementary measures as required. The parties agree that the EU Standard Contractual Clauses (2021/914) are incorporated by reference, Module 2 (Controller to Processor) applying where applicable, and are deemed executed upon execution of this DPA. CC shall provide details of the applicable transfer mechanism to You on request.

In the event that a transfer mechanism relied upon under this Clause 9 is invalidated by a court of competent jurisdiction, CC shall promptly substitute it for an alternative valid measure.

10. Upon receiving a verified deletion request from You (whether in response to a data subject request under Article 17 UK GDPR or otherwise), CC shall delete the relevant Alias (where one exists) within a reasonable timeframe. You acknowledge that:

(a) as Data Controller, it is Your responsibility to delete any mapping You hold that links Device Identifiers to identified individuals;

(b) once all Aliases held by CC and all mappings held by You in respect of the relevant data subject have been deleted, the remaining data held by CC constitutes Anonymised Data; and

(c) Anonymised Data is not Personal Data and may be retained by CC for analytical, product improvement, or other legitimate purposes.

11. The Parties agree that:

(a) Subject to any liability provisions in the Agreement, CC shall indemnify and keep indemnified You from and against any and all direct costs incurred by You under the Agreement in respect of any claims arising out of or in connection with CC's breach of its obligations under this DPA;

(b) You shall indemnify and keep indemnified CC from and against any and all direct costs incurred by CC under the Agreement in respect of any claims arising out of or in connection with Your breach of Your obligations

under this DPA, including any failure to maintain a lawful basis for processing or to fulfil Your obligations as Data Controller.

Nothing in this Clause 11 shall restrict or limit either Party's general obligation at law to mitigate a loss it may suffer or incur as a result of an event that may give rise to a claim under this indemnity.

The Parties agree that any liability arising under or in connection with this DPA (including under this Clause 11) shall be subject to the limitations of liability set out in the Agreement, provided that nothing in the Agreement or this DPA shall limit liability where such limitation is prohibited by applicable Data Protection Legislation or the applicable transfer mechanism.

12. The Parties hereby agree that they may enter into any additional binding agreement(s) supplemental to this DPA as are reasonably required to comply fully with Data Protection Legislation in any territory where Customer Data is being processed under the Agreement, whether under the direction of a Data Controller or otherwise (each a "**Supplemental Agreement**"). In the event of any conflict between any term or condition of a Supplemental Agreement and this DPA, the provisions of the Supplemental Agreement shall take precedence.

13. In the event of an actual or suspected Data Breach, CC will use all reasonable endeavours to provide You with an accurate written notice immediately upon becoming aware of it, and in no event later than within twenty-four (24) hours. CC shall work with Your prior approval on quickly resolving the issue, and prevent further losses, and provide any notices to an individual or government authority containing the information as mandated under applicable law.