DATA PROTECTION ADDENDUM

1 Definitions

1.1 In this Data Protection Addendum, the following terms have the meanings set out below unless the context otherwise requires:

Applicable Data Laws	as applicable and binding on the Customer, the Supplier and/or the Services: (a) in the United Kingdom: (i) the Data Protection Act 2018; and (ii) the GDPR, and/or any corresponding or equivalent national laws or regulations; (b) in member states of the European Union (**EU**) and/or European Economic Area (**EEA**): the GDPR and all relevant EU and EEA member state laws or regulations giving effect to or corresponding with any of the GDPR; and (c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Applicable Data Laws from time to time;
Applicable Law	applicable laws of the European Union (EU), the European Economic Area (EEA) or any of the EU or EEA's member states from time to time together with applicable laws in the United Kingdom from time to time*;*
Appropriate Safeguards	such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Applicable Data Laws from time to time;
Controller, **Data Subject**, **Personal Data**, **Personal Data Breach, processing** and **Processor**	have the meanings given to those terms and equivalent terms in Applicable Data Laws;
Data Protection Losses	means all liabilities, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and (iii) the reasonable costs of compliance with investigations by a Supervisory Authority;
Data Subject Request	a request made by a Data Subject to exercise any rights of Data Subjects under Applicable Data Laws;
GDPR	the General Data Protection Regulation, Regulation (EU) 2016/679;
International Organisation	an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
International Recipient	(a) any countries outside the United Kingdom and/or the European Economic Area; or (b) any International Organisation(s);
our Agreement	the agreement between the Supplier and the Customer for the provision of the Services (as updated from time to time) (including any Order Forms);
Privacy Policy	the InfoSum Privacy Policy available at https://www.infosum.com/legals/privacy-policy (as updated from time to

time);

Protected Data	Personal Data in the Uploaded Data;
Security Policy	the InfoSum Security Policy available at https://www.infosum.com/legals/security-policy (as updated from time to time)
Services	the services provided by the Supplier under our Agreement;
Sub-Processor	another Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Customer or an Authorised Affiliate (as updated by the Supplier from time to time), which as at the date of our Agreement are as set out in Annex A; and
Supervisory Authority	any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Applicable Data Laws.

1.2 Capitalised terms that are not separately defined (such as "**Account Data**", "**Affiliate**" "**Authorised Affiliates**", "**Individual User**", "**InfoSum Platform**", "**Order Form**", "**Platform Services**", "**Standard Pricing Terms**", "**Uploaded Data**", "**User**" and "**User Manual**" (or equivalent terms)) shall have the same meaning given to those terms in our Agreement.

2 Processor and Controller

2.1 The parties agree that, for the Protected Data, the Customer shall be the Controller and the Supplier shall be the Processor.

2.2 To the extent the Customer is not sole Controller of any Protected Data it warrants that it has full authority and authorisation of all relevant Controllers (including the Authorised Affiliates) to instruct the Supplier to process the Protected Data in accordance with our Agreement.

2.3 The Supplier shall process Protected Data in compliance with the obligations of Processors under Applicable Data Laws in respect of the performance of its and their obligations under our Agreement, and the terms of our Agreement.

2.4 The Customer shall ensure that it, its Affiliates and each Individual User shall at all times comply with:

2.4.1 all Applicable Data Laws in connection with the processing of Protected Data, the use of the Services (and each part) and the exercise and performance of its respective rights and obligations under our Agreement, including maintaining all relevant regulatory registrations and notifications as required under Applicable Data Laws; and

2.4.2 the terms of our Agreement.

2.5 The Customer warrants, represents and undertakes, that at all times:

2.5.1 all Protected Data (if processed in accordance with our Agreement) shall comply in all respects, including in terms of its collection, storage and processing, with Applicable Data Laws;

2.5.2 it is entitled to upload Personal Data and that such Personal Data has a valid legal basis for use within the InfoSum Platform; and

2.5.3 all Protected Data shall comply with the applicable provisions of our Agreement;

2.5.4 fair processing and other information notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by Applicable Data Laws in connection with all processing activities in respect of the Protected Data which may be undertaken by the Supplier and its Sub-Processors in accordance with our Agreement;

2.5.5 the Protected Data is accurate and up to date;

2.5.6 it shall establish and maintain adequate security measures to safeguard Protected Data in its possession or control from unauthorised access and copying and maintain complete and accurate backups of all Protected Data provided to the Supplier (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by the Supplier or any other person;

2.5.7 all instructions given by it to the Supplier in respect of Personal Data shall at all times be in accordance with Applicable Data Laws; and

2.5.8 it is satisfied that the Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Supplier to process the Protected Data.

3 Instructions and details of processing

3.1 Insofar as the Supplier processes Protected Data on behalf of the Customer, the Supplier:

3.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in in our Agreement (including this paragraph 3.1 and paragraphs 3.3.1 and 3.4), as updated from time to time, and via the InfoSum Platform (**Processing Instructions**);

3.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

3.1.3 shall promptly inform the Customer if the Supplier becomes aware of a Processing Instruction that, in the Supplier's opinion, infringes Applicable Data Laws, provided that:

(a) this shall be without prejudice to paragraphs 2.3, 2.4 and 2.5; and

(b) to the maximum extent permitted by mandatory law, the Supplier shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following the Customer's receipt of that information.

3.2 The Customer shall be responsible for ensuring all Authorised Affiliates and Individual Users read and understand the Privacy Policy (as updated from time to time).

3.3 The Customer acknowledges and agrees that:

3.3.1 the execution of any computer command to process (including deletion of) any Protected Data made in the use of any of the Platform Services by an Individual User will be a Processing Instruction authorised by the Customer or other relevant Controllers (other than to the extent such command is not fulfilled due to technical, operational or other reasons, including as set out in the User Manual); and

3.3.2 if any Protected Data is deleted pursuant to any such command the Supplier is under no obligation to seek to restore it.

3.4 Subject to the terms of our Agreement, the processing of the Protected Data by the Supplier under our Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in Annex A.

4 Technical and organisational measures

4.1 Taking into account the nature of the processing, the Supplier shall implement and maintain, at its cost and expense, the technical and organisational measures:

4.1.1 in relation to the processing of Protected Data by the Supplier, as set out the Security Policy; and

4.1.2 to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

5 Using staff and other processors

5.1 The Supplier shall not engage any Sub-Processor for carrying out any processing activities in respect of the Protected Data except in accordance with our Agreement without the Customer's written authorisation of that Sub-Processor (such authorisation not to be unreasonably withheld, conditioned or delayed).

5.2 The Customer authorises the appointment of each of the Sub-Processors listed in Annex A, which the Supplier may update from time to time, subject to clause 5.3.

5.3 The Supplier shall:

5.3.1 provide the Customer with an opportunity to object to any new Sub-Processors;

5.3.2 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under this Data Protection Addendum (as relevant to the specific processing services being performed) that is enforceable by the Supplier;

5.3.3 ensure each such Sub-Processor complies with all such obligations; and

5.3.4 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.4 The Supplier shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

6 Assistance with compliance and Data Subject rights

6.1 The Supplier shall:

6.1.1 refer all Data Subject Requests it receives to the Customer without undue delays:

6.1.2 provide such reasonable assistance as the Customer reasonably requires in responding to Data Subject Requests, provided that:

(a) the Customer acknowledges that the Platform Services are such that the Customer maintains access to its Uploaded Data and data generated from the Customer's use of the Platform Services, and the Customer will retain its own raw data; and

(b) in each case such support shall be provided, if requested by the Customer, by the Supplier, at the Customer's cost on a time and materials basis in accordance with the Supplier's Standard Pricing Terms.

6.2 The Supplier shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer's obligations under Applicable Data Laws with respect to:

6.2.1 security of processing;

6.2.2 data protection impact assessments (as defined in Applicable Data Laws);

6.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

6.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay the Supplier for all work, time, costs and expenses incurred in connection with providing the assistance in this paragraph 6.2, calculated on a time and materials basis at the Supplier's rates set out in the Supplier's Standard Pricing Terms.

7 International data transfers

7.1 The Supplier will (unless it notifies the Customer otherwise in writing) ensure that all data processing activities by the Supplier and its Sub-Processors in relation to Uploaded Data shall take place in the EEA or, if the United Kingdom ceases to be a member of the EEA, in the United Kingdom.

7.2 Subject to paragraph 7.3, the Supplier shall not transfer, or otherwise directly or indirectly disclose, any Protected Data to any International Recipient without the prior written consent of the Customer except where the Supplier is required to transfer the Protected Data by Applicable Law (and shall inform the Customer of that legal requirement before the transfer, unless those laws prevent it doing so).

7.3 The Customer agrees that for the purposes of the proper provision of the Services (including for the processing of Account Data):

7.3.1 the Supplier may transfer any Protected Data to any International Recipient; or

7.3.2 where the United Kingdom ceases to be a member of the EEA, the Supplier may continue to process Protected Data within the United Kingdom and transfer Protected Data between the United Kingdom and EEA countries and with International Recipients (as applicable),

provided all such transfers by the Supplier of Protected Data (and any onward transfer) shall (to the extent required under Applicable Data Laws) be effected by way of Appropriate Safeguards and in accordance with Applicable Data Laws; and

7.3.3 the provisions of our Agreement shall constitute the Customer's instructions with respect to transfers in accordance with paragraph 3.1.1.

7.4 The Customer acknowledges and agrees that:

7.4.1 due to the nature of cloud services, the Protected Data may also be transferred to other geographical locations in connection with use of the Service further to access and/or computerised instructions initiated by Individual Users; and

7.4.2 the Supplier does not control such processing and the Customer shall ensure that Individual Users (and all others acting on its behalf) only initiate the transfer of Protected Data to other geographical locations if Appropriate Safeguards are in place and that such transfer is in compliance with all Applicable Laws.

8 Information and audit

8.1 The Supplier shall maintain, in accordance with Applicable Data Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

8.2 The Customer may by written notice to the Supplier request information regarding the Supplier's compliance with the obligations placed on it under this Data Protection Addendum. On receipt of such request the Supplier shall provide the Customer (or auditors mandated by the Customer) with a copy of the latest third party certifications and audits to the extent made generally available to its customers (as Updated from time to time). Such copies are confidential to the Supplier and shall be Supplier's Confidential Information for the purposes of our Agreement.

8.3 The Supplier shall, on request by the Customer, in accordance with Applicable Data Laws, make available to the Customer such information as is reasonably necessary to demonstrate the Supplier's compliance with its obligations under this Data Protection Addendum and Article 28 of the GDPR (and under any Applicable Data Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose provided:

8.3.1 such audit, inspection or information request is reasonable, limited to information in the Supplier's (or any Sub-Processor's) possession or control and is subject to the Customer giving the Supplier reasonable prior notice of such audit, inspection or information request;

8.3.2 the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which the Customer or third party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure the Supplier is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this paragraph 8.3);

8.3.3 all costs of such audit or inspection or responding to such information request shall be borne by the Customer, and the Supplier's costs, expenses, work and time incurred in connection with such audit or inspection shall be reimbursed by the Customer on a time and materials basis in accordance with the Supplier's Standard Pricing Terms;

8.3.4 the Customer's rights under this paragraph 8.3 may only be exercised once in any consecutive 12 month period, unless otherwise required by a Supervisory Authority or if the Customer (acting reasonably) believes the Supplier is in breach of this Data Protection Addendum;

8.3.5 the Customer shall promptly (and in any event within two Business Days report any non-compliance identified by the audit, inspection or release of information to the Supplier;

8.3.6 the Customer shall ensure that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure required by Applicable Law);

8.3.7 the Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of the Supplier and each Sub-Processor; and

8.3.8 the Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any third party auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of the Supplier or any Sub-Processor whilst conducting any such audit or inspection.

9 Breach notification

1.2 In respect of any Personal Data Breach involving Protected Data, the Supplier shall, without undue delay notify the Customer of the Personal Data Breach, and provide the Customer with details of the Personal Data Breach.

10 Deletion of Protected Data and copies

1.3 Following the end of the provision of the Services (or part) relating to the processing of Protected Data the Supplier shall dispose of Protected Data in accordance with its obligations under our Agreement. The Supplier shall have no liability for any deletion or destruction of any such Protected Data undertaken in accordance with our Agreement.

11 Supplier liability and claims

11.1 The Supplier shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with our Agreement:

11.1.1 only to the extent caused by the processing of Protected Data under our Agreement and directly resulting from the Supplier's breach of our Agreement; and

11.1.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of our Agreement by the Customer (including in accordance with paragraph 3.1.3(b)).

11.2 If a party receives a compensation claim from a person relating to processing of Protected Data in connection with our Agreement or the Services, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

11.2.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

11.2.2 consult fully with the other party in relation to any such action but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under our Agreement for paying the compensation.

12 Customer obligations

12.1 The Customer agrees that it shall not:

12.1.1 provide excessive Uploaded Data other than that which is strictly necessary to use the Platform Services for the purposes contemplated by our Agreement;

12.1.2 upload any sensitive personal data, special categories of Personal Data, personal data relating to criminal convictions and offences or any patient, medical or other protected health information regulated by the Heath Insurance Portability and Accountability Act (as amended) of the United States of America, or similar national, federal or state laws, rules or regulations (**Sensitive Data**), or use the InfoSum Platform in such a way as to generate Sensitive Data, without the Supplier's prior written consent; and

12.1.3 except where another User has explicitly agreed to the Customer using their data for "tagging", attempt to single-out any individual in another User's data set, or attempt to associate any data from another User's data set with any individual in the Customer's own data set or in any other data the Customer holds or has access to.

ANNEX A
DATA PROCESSING DETAILS

Subject-matter of processing:

Performance of our respective rights and obligations under our Agreement and delivery and receipt of the Services under our Agreement.

Duration of the processing:

Until the earlier of final termination or final expiry of our Agreement (or the relevant Order Form), except as otherwise expressly stated in our Agreement.

Nature and purpose of the processing:

The Supplier shall carry out processing on the Customer's behalf:

- in accordance with the rights and obligations of the parties under our Agreement;*]*
- as reasonably required to provide the Services;*]*
- as initiated, requested or instructed by Individual Users in connection with their use of the Services, or by the Customer, in each case in a manner consistent with our Agreement*; and/or*
- in relation to each Platform Service, otherwise in accordance with the nature and purpose identified in our Agreement*;*

Type of Personal Data:

The Supplier shall process such Personal Data as the Customer uploads to the InfoSum Platform and any other Personal Data, as more particularly set out in our Agreement, and which the Customer controls through use of the user interface. This may include (as relevant) legal and other names, e-mail addresses, phone numbers, demographical information, marketing data, behavioural data and such other data as the Customer determines.

Categories of Data Subjects:

The Supplier shall process Personal Data in relation to such categories of Data Subjects as the Customer uploads to the InfoSum Platform and any other Personal Data, as more particularly set out in our Agreement, and which the Customer controls through use of the user interface. This may include (as relevant) Individual Users, employees, customers or other Data Subjects.

Sub-Processors

Provider	**Service**
Amazon Web Services	Servers / Hosting Services