DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Master Services Agreement or other similar agreement (the "**Agreement**") executed by and between Customer ("**Customer**" shall refer to the entity or any Affiliate of the entity bound by the Agreement) and Aforza Limited, on behalf of itself and its subsidiaries and affiliates ("**Aforza**"). This DPA shall govern the Processing of Personal Data by Aforza, and on behalf of Customer, in connection with Aforza's provision of the Services to Customer pursuant to the Agreement. The terms of this DPA prevail over any conflicting terms in the Agreement and in any other agreement(s) between the Parties, with the sole exception of the Standard Contractual Clause, as that term is defined below. Where the terms of this Agreement conflict with the terms of an applicable module of the Standard Contractual Clauses, the terms of the applicable module of the Standard Contractual Clauses shall control.

This DPA, along with the associated Attachments, shall be deemed executed, with an effective date as of the date of the Agreement and/or Order Form/Statement of Work to which it relates.

1. INTERPRETATION

1.1 In this DPA the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Aforza**" means Aforza Limited, a company incorporated in England and Wales with its registered address at 3rd Floor 1 Ashley Road, Altrincham, Cheshire, United Kingdom, WA14 2DT.

(b) "**Agreement**" means the Master Services Agreement entered into by and between the Parties.

(c) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, GDPR and the CCPA (as and where applicable).

(d) "**CCPA**" means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder.

(e) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(f) "**Customer Data**" means what is defined in the Agreement as "Customer Data", provided that such data is electronic data and information submitted by or for Customer to the Services. This DPA does not apply to Content or Non-Aforza Applications as defined in the Agreement

(g) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Personal Data and the Processing thereof.

(h) "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

(i) "**EEA**" means the European Economic Area.

(j) "**GDPR**" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("**UK GDPR**"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(k) "**Personal Data**" means "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws, where such data is Customer Data.

(l) "**Personal Data Breach**" means a breach of Aforza's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Aforza's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(m) "**Personnel**" means a person's employees, agents, consultants or contractors.

(n) "**Process**" or "**Processing**" and inflection thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(o) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

(p) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "EU Restricted Transfer"); and (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "UK Restricted Transfer"), which would be prohibited without a legal basis under Chapter V of the GDPR.

(q) "**Standard Contractual Clauses,**" or **SCCs,**" means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(r) "**Service Data**" means any data relating to the use, support and/or operation of the Services, which is collected directly by Aforza from and/or about users of the Services and/or Customer's use of the Service for use for its own purposes.

(s) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Aforza for Customer pursuant to the Agreement.

(t) "**Sub-Processor**" means any third party appointed by or on behalf of Aforza to Process Personal Data.

(u) "**Supervisory Authority**": (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office.

(v) "**UK Transfer Addendum**" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Mandatory Clauses included in Part 2 thereof (the "UK Mandatory Clauses").

1.2 In this DPA:

(a) the terms, "**business**," "**commercial purpose**," "**sell**" and "**service provider**" shall have the respective meanings given thereto in the CCPA; and "**personal information**" shall mean Personal Data that constitutes "personal information" governed by the CCPA; and

(b) unless otherwise defined in this DPA, all capitalized terms in this DPA shall have the meaning given to them in the Agreement.

2. SCOPE OF THIS DATA PROCESSING ADDENDUM

2.1 The front-end of this DPA applies generally to Aforza's Processing of Personal Data under the Agreement.

2.2 Annex 1 (European Annex) to this DPA applies only if and to the extent Aforza's Processing of Personal Data under the Agreement is subject to the GDPR.

2.3 Annex 2 (California Annex) to this DPA applies only if and to the extent Aforza's Processing of Personal Data under the Agreement is subject to the CCPA with respect to which Customer is a "business" (as defined in the CCPA).

3. PROCESSING OF CUSTOMER PERSONAL DATA

3.1 **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data in the course of providing the Services to Customer pursuant to the Agreement, Customer is the Controller, Aforza is a Processor and that Aforza will engage Sub-processors pursuant to Annex 1, clause 2 "Sub-processing" below.

3.2 **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws including any applicable requirement to provide notice to Data Subjects of the use of Aforza as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer represents that its use of the Services will not violate the rights of any Data Subject that has opted-out from the sale of or other disclosure of Personal Data, to the extent applicable under the CCPA, nor shall the use of the Services violate any rights of any Data Subject to the extent applicable under the Applicable Data Protection Laws.

3.3 **Aforza's Processing of Personal Data**. Aforza shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.4 **Details of the Processing**. The subject-matter of Processing of Personal Data by Aforza is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 to European Annex (Details of the Processing) to this DPA.

4. AFORZA PERSONNEL

Aforza shall take commercially reasonable steps to ascertain the reliability of any Aforza Personnel who Process Personal Data, and shall enter into written confidentiality agreements with all Aforza Personnel who Process Personal Data that are not subject to professional or statutory obligations of confidentiality.

5. SECURITY

5.1 Aforza shall implement and maintain technical and organizational measures in relation to Personal Data designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access as described in Annex 3 (Security Measures) (the "**Security Measures**").

5.2 Aforza may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Personal Data.

6. DATA SUBJECT RIGHTS

6.1 Aforza, taking into account the nature of the Processing of Personal Data, shall provide Customer with such assistance as may be reasonably necessary and technically feasible to assist Customer in fulfilling its obligations to respond to Data Subject Requests. If Aforza receives a Data Subject Request, Customer will be responsible for responding to any such request.

6.2 Aforza shall:

(a) promptly notify Customer if it receives a Data Subject Request; and

(a) not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Customer, except on the written instructions of Customer or as required by Applicable Data Protection Laws.

6.3 Operational clarifications:

(a) When complying with its transparency obligations under Clause 8.3 of the SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, Aforza's and its

licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

(b) Where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Aforza to notify any third-party controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer.

(c) For the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

(d) Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Aforza (at Aforza's then-current professional services rates) in Aforza's cooperation and assistance provided to Customer under this Section 6, and shall on demand reimburse Aforza any such costs incurred by Aforza.

7. PERSONAL DATA BREACH

Breach notification and assistance

7.1 Aforza shall notify Customer without undue delay upon Aforza's discovering a Personal Data Breach affecting Personal Data. Aforza shall provide Customer with information (insofar as such information is within Aforza's possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Aforza) to allow Customer to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. Aforza's notification of or response to a Personal Data Breach shall not be construed as Aforza's acknowledgement of any fault or liability with respect to the Personal Data Breach.

7.2 Aforza shall reasonably co-operate with Customer and take such commercially reasonable steps as may be directed by Customer to assist in the investigation of any such Personal Data Breach.

7.3 Customer is solely responsible for complying with notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breaches.

Notification to Aforza

7.4 If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, any Data Subject(s), the public or others under Applicable Data Protection Laws, to the extent such notice directly or indirectly refers to or identifies Aforza, where permitted by applicable laws, Customer agrees to:

(a) notify Aforza in advance; and

(b) in good faith, consult with Aforza and consider any clarifications or corrections Aforza may reasonably recommend or request to any such notification, which: (i) relate to Aforza's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

8. CUSTOMER'S RESPONSIBILITIES

8.1 Customer agrees that, without limiting Aforza's obligations under Section 5 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Aforza uses to provide the Services; and (d) backing up Personal Data.

8.2 Customer shall ensure:

(a) that there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Aforza of Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where applicable)); and

(b) that all Data Subjects have (i) been presented with all required notices and statements (including as required by Article 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Aforza of Personal Data.

8.3 Customer agrees that the Service, the Security Measures, and Aforza's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

8.4 Customer shall not provide or otherwise make available to Aforza any Personal Data that contains any (a) Social Security numbers or other government-issued identification numbers; (b) protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) health insurance information; (d) biometric information; (e) passwords to any online accounts; (f) credentials to any financial accounts; (g) tax return data; (h) any payment card information subject to the Payment Card Industry Data Security Standard; (i) Personal Data of children under 13 years of age; or (j) any other information that falls within any special categories of personal data (as defined in GDPR) and/or data relating to criminal convictions and offences or related security measures (together, "Restricted Data").

9. LIABILITY

The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this DPA and the SCCs (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the

Agreement; provided that, nothing in this Section 9 will affect any person's liability to Data Subjects under the third-party beneficiary provisions of the SCCs (if and as they apply).

10. SERVICE DATA

10.1 Customer acknowledges that Aforza may collect, use and disclose Service Data for its own business purposes, such as:

(a) for accounting, tax, billing, audit, and compliance purposes;
(b) to provide, improve, develop, optimize and maintain the Services;
(c) to investigate fraud, spam, wrongful or unlawful use of the Services; and/or
(d) as otherwise permitted or required by applicable law.

10.2 In respect of any such Processing described in Section 10.1, Aforza:

(a) independently determines the purposes and means of such Processing;

(b) shall comply with Applicable Data Protection Laws (if and as applicable in the context);

(c) shall Process such Service Data as described in Aforza's relevant privacy notices/policies (such as that shown at www.aforza.com/privacy-policy, as updated from time to time); and

(d) where possible, shall apply technical and organizational safeguards to any relevant Personal Data that are no less protective than the Security Measures.

10.3 For the avoidance of doubt, this DPA shall not apply to Aforza collection, use, disclosure or other Processing of Service Data, and Service Data does not constitute Personal Data.

11. CHANGE IN LAWS

Aforza may on notice vary this DPA to the extent that (acting reasonably) it considers necessary to address the requirements of Applicable Data Protection Laws from time to time, including by varying or replacing the SCCs in the manner described in Paragraph 6.6 of Annex 1 (European Annex).

12. INCORPORATION AND PRECEDENCE

12.1 This DPA shall be incorporated into and form part of the Agreement with effect from the Addendum Effective Date.

12.2 In the event of any conflict or inconsistency between:

(a) this DPA and the Agreement, this DPA shall prevail; or

(b) any SCCs entered into pursuant to Paragraph 6 of Annex 1 (European Annex) and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

Annex 1

European Annex

1. PROCESSING OF CUSTOMER PERSONAL DATA

1.1 The Parties acknowledge and agree that the details of Aforza's Processing of Personal Data under this DPA and the Agreement (including the respective roles of the Parties relating to such Processing) are as set out in Attachment 1 to Annex 1 (European Annex) to the DPA.

1.2 Where Aforza receives an instruction from Customer that, in its reasonable opinion, infringes the GDPR, Aforza shall inform Customer.

1.3 Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing of Personal Data by or on behalf of Aforza pursuant to or in connection with the Agreement shall be in strict compliance with the GDPR and all other applicable laws.

2. SUB-PROCESSING

2.1 Customer generally authorizes Aforza to appoint Sub-Processors in accordance with this Paragraph 2.

2.2 Aforza may continue to use those Sub-Processors already engaged by Aforza as at the date of this DPA (as those Sub-Processors are shown, together with their respective functions and locations, in Annex 4 (Authorized Sub-Processors).

2.3 Aforza shall give Customer prior written notice of the appointment of any proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor, by providing Customer with an updated copy of the Sub-Processor List via a 'mailshot' or similar bulk distribution mechanism sent via email to Customer's contact point as set out in Attachment 1 to Annex 1 (European Annex). If, within fourteen (14) days of receipt of that notice, Customer notifies Aforza in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Aforza shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Sub-Processor; and

(b) where: (i) such a change cannot be made within sixty (60) days from Aforza's receipt of Customer's notice; (ii) no commercially reasonable change is available; and/or (iii) Customer declines to bear the cost of the proposed change, then either Party may by written notice to the other Party with immediate effect terminate the Agreement, either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-Processor, as its sole and exclusive remedy.

2.4 If Customer does not object to Aforza's appointment of a Sub-Processor during the objection period referred to in Paragraph 2.3, Customer shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

2.5 With respect to each Sub-Processor, Aforza shall maintain a written contract between Aforza and the Sub-Processor that includes terms which offer at least an equivalent level of protection for Personal Data as

those set out in this DPA (including the Security Measures). Aforza shall remain liable for any breach of this DPA caused by a Sub-Processor.

2.6 Operational clarifications:

(a) The terms and conditions of this Paragraph 2 apply in relation to Aforza's appointment and use of Sub-Processors under the SCCs.

(b) Any approval by Customer of Aforza's appointment of a Sub-Processor that is given expressly or deemed given pursuant to this Paragraph 2 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Sub-Processors if and as required under Clause 8.8 of the SCCs.

3. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

3.1 Aforza, taking into account the nature of the Processing and the information available to Aforza, shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments and prior consultations with Supervisory Authorities which Customer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Personal Data by Aforza.

3.2 Operational clarification: Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Aforza (at Aforza's then-current professional services rates) in Aforza's provision of any cooperation and assistance provided to Customer under Paragraph 3.1, and shall on demand reimburse Aforza any such costs incurred by Aforza.

4. RETURN AND DELETION

4.1 Subject to Paragraph 4.2 and 4.3, upon the date of cessation of any Services involving the Processing of Personal Data (the "**Cessation Date**"), Aforza shall promptly cease all Processing of Personal Data for any purpose other than for storage or as otherwise permitted or required under this DPA.

4.2 **Return of Customer Data:** Subject to Paragraph 4.4, at any point during the term of a subscription, Customer may initiate an export of Customer Data directly from the SFDC Platform. Within twenty-five (25) days after the Cessation Date ("**Post-cessation Storage Period**"), Customer may request return of Customer Data submitted to the Services (to the extent such data has not been deleted by Customer and Customer has not deleted the Aforza managed package in the SFDC Platform). Customer will be able to retrieve such Customer Data via downloadable files in comma separated value (.csv) format and attachments in their native format from the SFDC Platform. The foregoing return of Customer Data may not be available if the Aforza managed package is removed prior to contract termination, as removing the package may begin the deletion process for associated Customer Data.

4.3 **Deletion of Customer Data**[1]. Except as stated below, after termination of all Services, Customer Data submitted to the Services is retained in inactive status within the Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers used to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Services, Aforza reserves the right to reduce the number of days it retains such data after contract termination and will update Customer in the event of such a change.

	Day 0	Day 0 – 30	Day 30 – 120	Day 121 - 211	Day 121 – 301
During Active Subscription Agreement Customer Data is available for export by Customer directly from SFDC Platform **at any time**	Subscription terminates	Data available for return to customer	Data inactive and no longer available	Data deleted or overwritten from production	Data deleted or overwritten from backups

For Sandboxes[2], as part of its system maintenance, SFDC may delete any Sandbox that Customer has not logged into for 150 consecutive days. Thirty or more days before any such deletion, SFDC will notify Customer (email acceptable) that the Sandbox will be deleted if Customer does not log into it during that 30-day (or longer) period. Deletion of a Sandbox shall not terminate Customer's Sandbox subscription; if a Sandbox is deleted during Customer's Sandbox subscription term, Customer may create a new Sandbox. The foregoing deletion of Customer Data for managed packages may not be available if the packages were removed prior to contract termination.

4.4 Aforza may retain Customer Data where permitted or required by applicable law, for such period as may be required by such applicable law, provided that Aforza shall:

(a) maintain the confidentiality of all such Customer Data; and

(b) Process the Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention.

4.5 Operational clarification: Certification of deletion of Personal Data as described in Clauses 8.5 and 16(d) of the SCCs, shall be provided only upon Customer's written request.

[1] This section does not apply to Scratch Orgs. As part of its system maintenance, SFDC will periodically delete any Scratch Org, including any associated data or Active Scratch Objects, as set forth in the Scratch Org Documentation. Deletion of an active Scratch Org shall not terminate Customer's Scratch Org subscription; if an active Scratch Org is deleted during Customer's Scratch Org subscription term, Customer may create a new active Scratch Org. Creation of new active Scratch Orgs count towards the daily scratch org limits set forth in the Scratch Org Documentation.

[2] Sandbox subscriptions are for testing and development use only, and not for production use.

5. AUDIT RIGHTS

5.1 Aforza shall make available to Customer on request, such information as Aforza (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA.

5.2 Subject to Paragraphs 5.3 to 5.8, in the event that Customer (acting reasonably) is able to provide documentary evidence that the information made available by Aforza pursuant to Paragraph 5.1 is not sufficient in the circumstances to demonstrate Aforza's compliance with this DPA, Aforza shall allow for and contribute to audits, including on premise inspections, by Customer or an auditor mandated by Customer in relation to the Processing of Personal Data by Aforza.

5.3 Customer shall give Aforza reasonable notice of any audit or inspection to be conducted under Paragraph 5.2 (which shall in no event be less than fourteen (14) days' notice) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury or disruption to Aforza's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Aforza's other customers or the availability of Aforza's services to such other customers).

5.4 Prior to conducting any audit, Customer must submit a detailed proposed audit plan providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Aforza will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Aforza security, privacy, employment or other relevant policies). Aforza will work cooperatively with Customer to agree on a final audit plan.

5.5 If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request ("**Audit Report**") and Aforza has confirmed in writing that there are no known material changes in the controls audited and covered by such Audit Report(s), Customer agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures.

5.6 Aforza need not give access to its premises for the purposes of such an audit or inspection:

(a) where an Audit Report is accepted in lieu of such controls or measures in accordance with Paragraph 5.5;

(b) to any individual unless they produce reasonable evidence of their identity;

(c) to any auditor whom Aforza has not approved in advance (acting reasonably);

(d) to any individual who has not entered into a non-disclosure agreement with Aforza on terms acceptable to Aforza;

(e) outside normal business hours at those premises; or

(f) on more than one occasion in any calendar year during the term of the Agreement, except for any audits or inspections which Customer is required to carry out under the GDPR or by a Supervisory Authority.

5.7 Nothing in this DPA shall require Aforza to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their customers.

5.8 Operational clarifications:

(a) Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Aforza (at Aforza's then-current professional services rates) in Aforza's provision of any cooperation and assistance provided to Customer under this Paragraph 5 (excluding any costs incurred in the procurement, preparation or delivery of Audit Reports to Customer pursuant to Paragraph 5.5), and shall on demand reimburse Aforza any such costs incurred by Aforza.

(b) The audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in this Paragraph 5.

6. RESTRICTED TRANSFERS

EU Restricted Transfers

6.1 To the extent that any Processing of Personal Data under this DPA involves an EU Restricted Transfer from Customer to Aforza, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be:

(a) populated in accordance with Part 1 of Attachment 2 to Annex 1 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

UK Restricted Transfers

6.2 To the extent that any Processing of Personal Data under this DPA involves a UK Restricted Transfer from Customer to Aforza, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be:

(a) varied to address the requirements of the UK GDPR in accordance with UK Transfer Addendum and populated in accordance with Part 2 of Attachment 2 to Annex 1 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

Adoption of new transfer mechanism

6.3 Aforza may on notice vary this DPA and replace the relevant SCCs with:

(a) any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly (e.g., standard data protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the EU GDPR); or

(b) another transfer mechanism, other than the SCCs that enables the lawful transfer of Personal Data to Aforza under this DPA in compliance with Chapter V of the GDPR.

Provision of full-form SCCs

6.4 In respect of any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject or further Controller (where applicable) – on specific written request (made to the contact details set out in Attachment 1 to this Annex 1 (European Annex); accompanied by suitable supporting evidence of the relevant request), Aforza shall provide Customer with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with Attachment 2 to Annex 1 (European Annex) in respect of the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage to evidence Customer's compliance with Applicable Data Protection Laws.

ATTACHMENT 1 TO EUROPEAN ANNEX

Data Processing Details

Note: This Attachment 1 to Annex 1 (European Annex) to the DPA includes certain details of the Processing of Personal Data as required:

- by Article 28(3) GDPR; and
- to populate the Appendix to the SCCs in the manner described in Attachment 2 to Annex 1 (European Annex) to the DPA.

CUSTOMER / 'DATA EXPORTER' DETAILS

Name:	The Customer identified in the Agreement and/or Order Form(s)/Statement of Work and, all Affiliates of Customer.
Address:	Customer's address as identified in the Agreement and/or Order Form(s)/Statement(s) of Work.
Contact Details for Data Protection:	Customer's telephone number and email address, as identified in the Agreement and/or Order Form(s)/Statement of Work.
Customer Activities:	Customer's activities relevant to this DPA are the use and receipt of the Services under and in accordance with, and for the purposes anticipated and permitted in, the Agreement as part of its ongoing business operations.
Role:	• Controller - in respect of any Processing of Personal Data in respect of which Customer is a Controller in its own right; and • Processor – in respect of any Processing of Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person (including its affiliates if and where applicable).

AFORZA / 'DATA IMPORTER' DETAILS

Name:	Aforza Limited,
Address:	3rd Floor, 1 Ashley Road, Altrincham, Cheshire, WA14 2DT, United Kingdom
Contact Details for Data Protection:	Nick Eales, Chief Product Officer; privacy@aforza.com
Aforza Activities:	Performance of the Services pursuant to the Agreement and as further described in the Documentation.
Role:	Processor

DETAILS OF PROCESSING

Categories of Data Subjects:	Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: ● Prospects, customers, suppliers, service partners, direct or indirect distributors, resellers, sales agents, introducers, sales representatives, collaborators, joint venturers, business partners, vendors, (sub-)licensees and other providers of goods or services (who are natural persons) ● Employees or contact persons of prospects, customers, suppliers, service partners, direct or indirect distributors, resellers, sales agents, introducers, sales representatives, collaborators, joint venturers, business partners, vendors, (sub-)licensees and other providers of goods or services. ● Employees, agents, advisors, freelances of Customer (who are natural persons). ● Customer's Users authorized by Customer to use the Services ● End-users, consumers and/or other users of Customer's products and services ● Shareholders, investors, partners, members and supporters. ● Advisers, consultants and other professionals and experts. Where any of the above is a business or organization, it includes their staff, namely, employees and non-employee workers; students, interns, apprentices and volunteers; directors and officers; advisers, consultants, independent contractors, agents and autonomous, temporary or casual workers, together with applicants and candidates for any one or more of the foregoing roles or positions. Each category includes current, past and prospective Data Subjects.
Categories of Personal Data:	Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: ● First and last name ● Title ● Position ● Employer ● Contact information (company, email, phone, physical business address) ● ID data ● Professional life data ● Personal life data ● Localization data ● Technological data – for example internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise

	location data, internet / application / device / program activity data, and device IDs and addresses.
Sensitive Categories of Data, and associated additional restrictions/safeguards:	Categories of sensitive data: None – as noted in Section 8.4 of the DPA, Customer agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the SCCs), must not be submitted to the Services. Additional safeguards for sensitive data: Not Applicable
Frequency of transfer:	Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.
Nature of the Processing:	Processing operations required in order to provide the Services in accordance with the Agreement.
Purpose of the Processing:	Personal Data will be processed: (i) as necessary to provide the Services as initiated by Customer in its use thereof, and (ii) to comply with any other reasonable instructions provided by Customer in accordance with the terms of this DPA.
Duration of Processing / Retention Period	For the period determined in accordance with the Agreement and DPA, including Paragraph 4 of Annex 1 (European Annex) to the DPA.
Transfers to (sub) processors	Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List (as may be updated from time to time in accordance with Paragraph 2 of Annex 1 (European Annex) to the DPA).

ATTACHMENT 2 TO EUROPEAN ANNEX

POPULATION OF SCCs

Notes:

- In the context of any EU Restricted Transfer, the SCCs populated in accordance with Part 1 of this Attachment 2 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 6.2 of Annex 1 (European Annex) to the DPA).

- In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and populated in accordance with Part 2 of this Attachment 2 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 6.3 of Annex 1 (European Annex) to the DPA).

PART 1: POPULATION OF THE SCCs

1. SIGNATURE OF THE SCCs:

Where the SCCs apply in accordance with Paragraph 6.2 of Annex 1 (European Annex) to the DPA each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. MODULES

The following modules of the SCCs apply in the manner set out below (having regard to the role(s) of Customer set out in Attachment 1 to Annex 1 (European Annex) to the DPA):

(a) Module Two of the SCCs applies to any EU Restricted Transfer involving Processing of Personal Data in respect of which Customer is a Controller in its own right; and/or

(b) Module Three of the SCCs applies to any EU Restricted Transfer involving Processing of Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person.

3. POPULATION OF THE BODY OF THE SCCs

3.1 For each Module of the SCCs, the following applies as and where applicable to that Module and the Clauses thereof:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 9:

(i) OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Paragraph 2.3 of Annex 1 (European Annex) to the DPA; and

(ii) OPTION 1: SPECIFIC PRIOR AUTHORISATION is not used and that optional language is deleted; as is, therefore, Annex III to the Appendix to the SCCs.

(c) In Clause 11, the optional language is not used and is deleted.

(d) In Clause 13, all square brackets are removed and all text therein is retained.

(e) In Clause 17: OPTION 1 applies, and the Parties agree that the SCCs shall be governed by the law of Ireland in relation to any EU Restricted Transfer; and OPTION 2 is not used and that optional language is deleted.

(f) For the purposes of Clause 18, the Parties agree that any dispute arising from the SCCs in relation to any EU Restricted Transfer shall be resolved by the courts of Ireland, and Clause 18(b) is populated accordingly.

3.2 In this Paragraph 3, references to "**Clauses**" are references to the Clauses of the SCCs.

4. POPULATION OF ANNEXES TO THE APPENDIX TO THE SCCs

4.1 Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Attachment 1 to Annex 1 (European Annex) to the DPA, with: Customer being 'data exporter'; and Aforza being 'data importer'.

4.2 Part C of Annex I to the Appendix to the SCCs is populated as the Information Commissioner's Office.

4.3 Annex II to the Appendix to the SCCs is populated as below:

General:

- Please refer to Section 5 of the DPA and Annex 3 (Security Measures) to the DPA.
- In the event that Customer receives a Data Subject Request under the EU GDPR and requires assistance from Aforza, Customer should email Aforza's contact point for data protection identified in Attachment 1 to Annex 1 (European Annex) to the DPA.

Sub-Processors: When Aforza engages a Sub-Processor under these Clauses, Aforza shall enter into a binding contractual arrangement with such Sub-Processor that imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the DPA – including in respect of:

- applicable information security measures;
- notification of Personal Data Breaches to Aforza;
- return or deletion of Personal Data as and where required; and engagement of further Sub-Processors.

PART 2: UK RESTRICTED TRANSFERS

1. UK TRANSFER ADDENDUM

1.1 Where relevant in accordance with Paragraph 6.3 of Annex 1 (European Annex) to the DPA, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below –

(a) *Part 1 to the UK Transfer Addendum*. The Parties agree:

(i) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Attachment 1 to Annex 1 (European Annex) to the DPA and the foregoing provisions of this Attachment 2 (subject to the variations effected by the UK Mandatory Clauses described in (b) below); and

(ii) Table 4 to the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.

(b) *Part 2 to the UK Transfer Addendum*. The Parties agree to be bound by the UK Mandatory Clauses of the UK Transfer Addendum.

1.2 As permitted by Section 17 of the UK Mandatory Clauses, the Parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Transfer Addendum in the manner set out in Paragraph 1.1 of this Part 2; **provided that** the Parties further agree that nothing in the manner of that presentation shall operate or be construed so as to reduce the Appropriate Safeguards (as defined in Section 3 of the UK Mandatory Clauses).

1.3 In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in Paragraph 1.1 of this Part 2.

Annex 2

California Annex

1. Aforza shall not retain, use, or disclose any Personal Data that constitutes "personal information" under the CCPA ("**CA Personal Information**") for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by CCPA, including retaining, using, or disclosing the CA Personal Information for a commercial purpose other than providing the Services.

2. Aforza shall not (a) sell any CA Personal Information; (b) retain, use or disclose any CA Personal Information for any purpose other than for the specific purpose of providing the Service, including retaining, using, or disclosing the CA Personal Information for a commercial purpose other than provision of the Services; or (c) retain, use or disclose the CA Personal Information outside of the direct business relationship between Aforza and Customer. Aforza hereby certifies that it understands its obligations under this Annex 2 and will comply with them.

3. It is the Parties' intent that with respect to any CA Personal Information, Aforza is a service provider.

4. Provision of the Services encompasses the Processing authorized by Customer's instructions described in the DPA. The Parties acknowledge that Aforza's retention, use and disclosure of CA Personal Information authorized by Customer's instructions are integral to Aforza's provision of the Services and the business relationship between the Parties.

5. Notwithstanding anything in the Agreement or any order form entered in connection therewith, the Parties acknowledge and agree that Aforza's access to CA Personal Information or any other Personal Data does not constitute part of the consideration exchanged by the Parties in respect of the Agreement.

Annex 3

Security Measures

As from the Addendum Effective Date, Aforza will implement and maintain the Security Measures as set out in this Annex 3.

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Aforza's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Aforza's organization, monitoring and maintaining compliance with Aforza's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to protect information assets from unauthorized physical access or damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Aforza's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Aforza's technology and information assets.

10. Incident management procedures designed to allow Aforza to investigate, respond to, mitigate and notify of events related to Aforza's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Aforza may freely update or modify these Security Measures from time to time **provided that** such updates and modifications do not decrease the overall security of Personal Data.

Annex 4

Authorized Sub-Processors

Sub-Processor:	Function:	Entity Location:
Google Cloud Platform; Google LLC	Third party hosting provider	USA
Jira Software (Atlassian PTY Ltd)	Third party code development, testing and ticketing system	USA
Mapbox, Inc	Third party map visualization provider	USA
Mixpanel, Inc	Third party provider for analyzing mobile application user behaviour	USA
Open AI, LLC	Third party provider of generative artificial intelligence services	USA
Okta, Inc	Third party authentication provider	USA
Salesforce.com	Third party hosting provider	USA
Functional Software, Inc d/b/a Sentry	Third party provider for tracking analyzing mobile application performance	USA
Workato, Inc	Third party integration and automated workflow provider	USA