DATA PROCESSING AGREEMENT

This Data Processing Agreement, including its attached schedules and appendices, ("**DPA**") is a part of and subject to the master services agreement between the relevant Forsta entity ("**Forsta**") and corresponding client entity ("**Client**") (collectively, the **"Parties"**, each a "**Party**") for the purchase of services from Forsta that references these terms (the "**Agreement**").

The Parties agree:

Capitalized terms in this DPA shall have the same meaning set out in the Agreement unless otherwise stated herein. If Forsta processes Personal Data for an Affiliate of Client, by entering into this DPA, Client enters into this DPA on behalf of itself and its Affiliate. In such case, the term "Client" shall include Client and such Affiliate.

1. Definitions

The following capitalized terms have the following meanings:

1.1. "**Applicable Data Privacy Law**" refers to all laws and regulations applicable to Forsta's processing of personal data under the Agreement.

1.2. "**controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.3. "**Business Data**" means personal data shared between the parties for the purposes of doing business together, but not in relation to the actual use of the Services, including, but not limited to, the personal data of Client's personnel who negotiate agreements between the parties, administer Client's financial account with Forsta, or discuss new services for purchase from Forsta.

1.4. "**Client Data**" means (a) any personal data furnished to Forsta by Client (or on behalf of Client) in relation to using the Services, including, but not limited to survey responses, questionnaire responses, reports, e-mail addresses, information, content, images, files, data, voice and video media, images, email bodies, email recipients, sound, and, where applicable, details Client submits to the Services from its designated software applications and services and (b) data stored on Client's behalf such as communication logs within the Services or marketing campaign data that Client has uploaded to the Services. For clarity, this does not include Business Data.

1.5. "**Forsta Privacy Notice**" means the privacy notice which is available at https://legal.forsta.com/legal/privacy-notice/ or such other URL as determined by Forsta.

1.6. "**personal data**" means any information relating to an identified or identifiable natural person ("**data subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.7. "**processor**" means the entity which processes personal data on behalf of the Client.

1.8. "**processing**" (and "**process**") means any operation or set of operations 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.

1.9. "**Security Incident**" means an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data.

1.10. "**Sensitive Data**" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), financial information, banking account numbers or passwords; (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about

sexual life or sexual orientation; (e) account passwords, mother's maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of "special categories of data" under GDPR or any other Applicable Data Privacy Law.

1.11. "**Services**" means the products and services provided by Forsta or its Affiliates, as applicable, that are (a) used by Client, including, without limitation, products and services that are on a trial basis or otherwise free of charge or (b) ordered by Client under a Sales Order or other commercial document.

1.12. "**sub-processor**" means (a) Forsta, when Forsta is processing Client Data and where Client is a processor of such Client Data or (b) any third-party processor engaged by Forsta to process Client Data in order to provide the Services to Client. For the avoidance of doubt, telecommunication providers are not sub-processors.

1.13. "**Usage Data**" means data generated by a user's use of the Services and may include information such as a computer's Internet Protocol address (e.g. IP address), browser type, browser version, the time and date of the use, the time spent using certain parts of the Services, unique device identifiers, and other diagnostic data.

2. Relationship of the Parties

2.1. Forsta as a Processor. Regarding the processing of Client Data, Client could be either a controller or processor, and Forsta is a processor on behalf of the Client. Forsta will process Client Data as described in this DPA.

2.2. Forsta as a Controller of Usage Data. Regarding the processing of Usage Data, Forsta is a controller of such Usage Data and Client does not own or have any right in such Usage Data. Client warrants that its Authorized Users are noticed of the contents of the Forsta Privacy Notice. Forsta will process Usage Data in accordance with the Forsta Privacy Notice and not according to this DPA.

2.3. Forsta as a Controller of Business Data. Regarding the processing of Business Data, Forsta is a controller and Client's personnel are the data subjects. Such processing is subject to Forsta's data protection practices which are detailed in the Forsta Privacy Notice. For clarity, Business Data may be Confidential Information for the purposes of the Agreement and the treatment of Confidential Information may be detailed in the Agreement. Forsta will process Business Data in accordance with the Forsta Privacy Notice and not according to this DPA.

3. Instructions

3.1. Forsta will only process personal data on documented instructions from the Client (unless required to do so by a law to which Forsta is subject), contained herein and in written communications between the Parties. For the avoidance of doubt, Client's use of Forsta's Services will constitute written communication to process personal data as necessary to facilitate such intended use as described in the Documentation. In the case of processing required by law, Forsta shall inform the Client of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

3.2. Lawfulness of Instructions. Client will ensure that its instructions comply with Applicable Data Privacy Law. Forsta shall immediately inform the Client if, in Forsta's opinion, instructions given by the Client infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions or if required to do by Applicable Data Privacy Law.

3.3. Additional Instructions. Additional instructions outside the scope of the Agreement or this DPA will be agreed to between the parties in writing, including any additional fees that may be payable by Client to Forsta for carrying out such additional instructions.

4. Purpose Limitation

4.1. Forsta shall process the personal data only for the specific purpose(s) of the processing, as set

out in Schedule I, unless it receives further instructions from the Client.

5. Duration of Processing

5.1. Processing by Forsta shall only take place during the term of Agreement between the Parties or such further time as required by Applicable Data Privacy Law.

6. Compliance, Information Distribution, Audits

6.1. Certification. This DPA shall serve as a certification that Forsta understands the requirements of Applicable Data Privacy Law and will comply with those requirements.

6.2. Compliance with law. Client is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Privacy Law in its use of the Services and its own processing of personal data and (b) it has, and will continue to have, the right to transfer, or provide access to, personal data to Forsta for processing in accordance with the terms of the Agreement and this DPA. Client will ensure that its instructions comply with Applicable Data Privacy Law. Client acknowledges that Forsta is neither responsible for determining which laws or regulations are applicable to Client's business nor whether Forsta's provision of the Services meets or will meet the requirements of such laws or regulations. Client will ensure that Forsta's processing of Client Data, when done in accordance with Client's instructions, will not cause Forsta to violate any applicable law or regulation, including Applicable Data Privacy Law.

6.3. To provide Client with information necessary to assist Client in Client's efforts to comply with applicable data protection legislation and to respond to inquiries from data protection authorities and data subjects, Forsta shall, upon Client's request and at no cost to Client, provide Client with (i) all information required to be provided by Forsta by law; (ii) Forsta's standard security documentation; (iii) available summaries of application and vulnerability scans of the Service; (iv) records of processing activities; and (v) responses to follow-up questions in relation to the foregoing. Any assistance beyond the foregoing, such as, but not limited to, Forsta's further assistance to Client in relation to Client's security audits and reviews, notification obligations, data protection impacts assessments, consultation with data protection authorities, and exercise of data subject rights pursuant to applicable law, shall be subject to terms and costs to be agreed mutually in writing between the Parties.

6.4. Data Subject Rights. If either party receives any request from a data subject to exercise any of its rights under Applicable Data Privacy Law or any third-party request relating to the processing of Client Data conducted by the other party, such party will promptly inform such other party in writing. The parties agree to cooperate, in good faith, as described herein to respond to any third-party request and fulfill their respective obligations under Applicable Data Privacy Law.

6.4.1. To the extent Client does not have the ability to resolve a data subject request through any of the self-service features available in the Services, upon Client's request, Forsta will provide reasonable additional and timely assistance to assist Client in complying with its data protection obligations with respect to data subject rights under Applicable Data Privacy Law.

6.5. Audit. Forsta will audit its compliance with its security obligations hereunder using industry standard methods and may use a third party to do so. Forsta will perform such audits at least once annually at Forsta's expense to result in the generation of a confidential audit report ("Audit Report"). Upon Client's written request at reasonable intervals, and subject to reasonable confidentiality controls, Forsta will make available to Client a summary of Forsta's most recent Audit Report. If a summary of such report does not provide sufficient information to meet Forsta's obligations under Applicable Data Privacy Law, Forsta may provide a copy of the most recent Audit Report, subject to reasonable confidentiality controls.

6.6. Client Audit. To the extent that Forsta's provision of a summary or copy of its most recent Audit Report does not provide sufficient information to meet its obligations under Applicable Data Privacy Law, Client may audit Forsta's compliance with its obligations hereunder to the extent required by Applicable Data Privacy Law if Client (a) ensures the use of an independent third

party without a conflict of interest with Forsta; (b) provides written notice to Forsta in a timely fashion no less than 60 days in advance; (c) requests access only during business hours and only to Forsta's global headquarters (currently the headquarters of Press Ganey Associates LLC); (d) accepts billing to Client at Forsta's then-current rates for use of its personnel; (e) exercises this right no more than once every 12 months (inclusive of all other audit rights exercised under the Agreement); (f) restricts its findings to only data relevant to Client; and (g) obligates its personnel, to the extent permitted by law or regulation, to keep confidential any information gathered.

6.7. Assessments. To the extent that Forsta's provision of a summary or copy of its most recent Audit Report does not provide sufficient information to meet its obligations under Applicable Data Privacy Law, Forsta will reasonably assist the Client with its obligation to

6.7.1. carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons; and

6.7.2. consult the competent supervisory authority(ies) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

7. Security, Confidentiality, Breach Notification

7.1. Forsta will implement the technical and organizational measures specified in Schedule II ("Forsta TOMs") for processing Client Data. Forsta will design Forsta TOMs to protect personal data uploaded into its services, taking into account the state of the art, the costs of implementation and the most likely 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; however, Client will only use the Services if it has made an independent determination that proper implementation of Forsta TOMs and available configuration of the Services guarantee that the processing described in Schedule I will meet the requirements of Applicable Data Privacy Law. Client will review the information Forsta makes available regarding its data security, including its audit reports. Client will configure the Services and use features and functionalities made available by Forsta to maintain appropriate security in light of the nature of Client Data processed as a result of Client's instructions. Forsta will provide reasonable assistance in the configuration of the Software settings or current features for the purposes of security of personal data.

7.2. Forsta will take steps to ensure that any natural person acting under the authority of Forsta who has access to personal data does not process them except on instructions from the Client, unless he or she is required to do so by law. Further, Forsta will ensure that persons authorized to process the personal data received have committed themselves to confidentiality obligations at least as protective as those contained herein or are under an appropriate statutory obligation of confidentiality that is at least as protective as the obligations of Forsta herein.

7.3. Security Incident notification. Forsta will provide notification of a Security Incident in the following manner:

7.3.1. Forsta will, to the extent permitted by applicable law, notify Client (and, for clarity, not the data subject, unless required to by Applicable Data Privacy Law) without undue delay after Forsta having become aware of a Security Incident impacting Client Data of which Forsta is a processor; and

7.3.2. Forsta will notify Client of such Security Incident via email to the email address(es) designated by Client in Client's account.

7.3.3. Such notification of a Security Incident will contain, at least:

7.3.3.1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

7.3.3.2. the details of a contact point where more information concerning the Security Incident can be obtained;

7.3.3.3. its likely consequences and the measures taken or proposed to be taken to address

the breach, including to mitigate its possible adverse effects.

7.3.4. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided by Forsta without undue delay.

7.4. Forsta will make reasonable efforts to identify Security Incidents and, to the extent a Security Incident is caused by Forsta's violation of this DPA, remediate the cause of such breach. Forsta will provide reasonable assistance to Client in the event that Client is required under Applicable Data Privacy Law to notify a regulatory authority or any data subjects impacted by a Security Incident.

8. Sensitive data

8.1. If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences or other categories of data deemed 'sensitive' under Applicable Data Privacy Law ("sensitive data"), Client warrants that it has instructed Forsta to process such data according to the necessary additional safeguards that may be required under Applicable Data Privacy Law via Forsta's technical and organizational measures described herein.

9. Sub-processors

9.1. General Authorization. Client authorizes Forsta to engage sub-processors generally, conditioned on the following requirements:

9.1.1. Forsta will restrict the onward sub-processor's access to Client Data only to what is strictly necessary for the purposes listed in Schedule I; and Forsta will prohibit the sub-processor from processing the personal data for any other purpose.

9.1.2. Forsta agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Client Data to the standard required by Applicable Data Privacy Law, including the requirements set forth in Schedule IV (Jurisdiction Specific Terms) of this DPA, which may include adequate transfer mechanisms, if required.

9.1.3. Forsta will remain liable for any breach of this DPA that is caused by an act, error, or omission of its sub-processors.

9.2. Current Sub-processors and Notification of Sub-processor Changes. Forsta will maintain an up-to-date list of its sub-processors at https://legal.forsta.com/legal/forsta-sub-processor-list/ (or such other URL as determined by Forsta from time to time). A change to such list is considered the notice of sub-processor changes required by Applicable Data Privacy Law (there will be a mechanism on such website to receive notice via email when a change has occurred). With respect to changes in infrastructure providers, Forsta will endeavor to give written notice 60 days prior to any change, but in any event will give written notice no less than 30 days prior to any such change. With respect to Forsta's other sub-processors, Forsta will endeavor to give written notice 30 days prior to any change but will give written notice no less than 10 days prior to any such change.

9.3. Objection Right for new Sub-processors. Client may object to Forsta's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection and made in good faith. In such an event, the parties agree to discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach a resolution within 90 days' notice or within the time when the intended changes are to be implemented, Client shall, without penalty (notwithstanding any term in the Agreement), upon written notice, terminate the Agreement to the extent that it obligates Forsta to provide and for Client to pay for the Services affected by the objection. Such termination will be without prejudice to any fees incurred by

Client prior to the termination. If no objection has been raised prior to Forsta replacing or appointing a new sub-processor, the Client will be deemed to have authorized the new sub-processor.

10. International Provisions

10.1. Jurisdiction Specific Terms. To the extent Forsta processes personal data originating from and protected by Applicable Data Privacy Law in one of the jurisdictions listed in Schedule IV (Jurisdiction Specific Terms) of this DPA, the terms specified in Schedule IV with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

10.2. Cross Border Data Transfer Mechanisms for Data Transfers. To the extent Client's use of the Services requires a transfer mechanism to lawfully transfer personal data protected by the laws of a jurisdiction (i.e., the European Economic Area, the United Kingdom, Switzerland, or any other jurisdiction listed in Schedule IV (Jurisdiction Specific Terms) of this DPA) to Forsta being incorporated outside of that jurisdiction ("*Transfer Mechanism*"), the terms set forth in Schedule III (Cross Border Transfer Mechanisms) of this DPA will apply.

11. Miscellaneous

11.1. Return or Deletion of Client Data. Forsta will delete or return to Client any Client Data stored within the Services after the duration of processing described in Schedule I.

11.2. Extension of DPA. Upon termination of the Agreement, Forsta may retain Client Data in storage for the time periods set forth in Schedule I (Details of Processing) of this DPA, provided that Forsta will ensure that Client Data (a) is processed only as necessary for the purposes described in Schedule I and (b) remains protected in accordance with the terms of the Agreement, this DPA, and Applicable Data Privacy Law.

11.3. Retention Required by Law. Notwithstanding anything to the contrary in this Section, Forsta may retain Client Data, or any portion of it, if required by applicable law or regulation, including Applicable Data Privacy Law, provided such Client Data remains protected in accordance with the terms of the Agreement, this DPA, and Applicable Data Privacy Law.

11.4. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule IV (Jurisdiction Specific Terms) of this DPA; (2) the terms of this DPA outside of Schedule IV (Jurisdiction Specific Terms); (3) the Agreement; and (4) the Forsta Privacy Notice. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, without limitation, the exclusions and limitations set forth in the Agreement.

11.5. Updates. Forsta may update the terms of this DPA from time to time upon at least thirty (30) days prior written notice only if an update is required as a result of (a) changes in Applicable Data Privacy Law; (b) a merger, acquisition, or other similar transaction involving Forsta; or (c) the release of new products or services or material changes to any of the existing Services. The then-current terms of this DPA are available at https://legal.forsta.com/legal/forsta-data-processing-agreement/.

SCHEDULE I
DETAILS OF PROCESSING

1. **Nature and Purpose of the Processing**. Forsta will process personal data as necessary to provide the Services under the Agreement. Forsta does not sell Client's personal data or Client end users' personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.
   1.1. Client Data. Forsta will process Client Data as a processor in accordance with Client's instructions as set forth in this DPA.
   1.2. Usage Data. Forsta will process Usage Data as a controller as described in the Forsta Privacy Notice and not according to this DPA.
   1.3. Business Data. Forsta will process Business Data as a controller as described in the Forsta Privacy Notice and not according to this DPA.
2. **Processing Activities**.
   2.1. Personal data contained in Client Data will be subject to the following basic processing activities:
      2.1.1. Ensuring uptime and security;
      2.1.2. Conducting support, maintenance, and error-correction;
      2.1.3. Verifying Client's compliance with the Agreement;
      2.1.4. The performance of other activities such as taking back-ups of data; and
      2.1.5. Storage of personal data on Forsta's network
      2.1.6. the provision of products and services which allows Client to integrate, manage and control its data relating to end users and respondents.
3. **Duration of the Processing**. The period for which personal data will be retained and the criteria used to determine that period is as follows:
   3.1. Prior to the termination of the Agreement, Forsta will process stored Client Data for the purposes described herein until Client elects to delete such Client Data via the Services and Client agrees that it is solely responsible for deleting Client Data via the Services.
   3.2. Upon termination of the Agreement, Forsta will (i) automatically delete any stored Client Data 60 business days after the termination effective date; and (ii) automatically delete any stored Client Data on Forsta's back-up systems up to 52 weeks after the termination effective date. Any Client Data archived on Forsta's back-up systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.
4. **Categories of Data Subjects**.
   4.1. The categories of data subjects are determined by the Client throughout the term of the Agreement but may include its end users which may be the employees or clients of Client.
5. **Categories of Personal Data**.
   5.1. The categories of personal data are determined by the Client throughout the term of the Agreement but may include the opinions of Client's end users about Client's workplace or services.
6. **Sensitive Data or Special Categories of Data**.
   6.1. Client Data. Client or its end users may choose to include Sensitive Data within data that is collected via the Services. Client is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Client's end users to transmit or process, any Sensitive Data via the Services.
7. **Sub-Processors**
   7.1. The subject matter, nature, and duration of the processing carried out by Forsta's sub-processors are the same as those by Forsta itself.

SCHEDULE II
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Description of the technical and organizational security measures implemented by Forsta to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

Found at https://legal.forsta.com/legal/forsta-technical-and-organizational-measures/, as updated from time to time.

Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the data exporter.

When Forsta engages a sub-processor under this DPA, Forsta and the sub-processor enter into an agreement with data protection obligations substantially similar to those contained in this DPA. Each sub-processor agreement must ensure that Forsta is able to meet its obligations to Client. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify Forsta in the event of a Security Incident so Forsta may notify Client; (b) delete personal data when instructed by Forsta in accordance with Client's instructions to Forsta; (c) not engage additional sub-processors without Forsta's authorization; d) use appropriate transfer mechanisms that are adequate under Applicable Data Privacy Law when required; and (e) process personal data in a manner which does not conflict with Client's instructions to Forsta.

SCHEDULE III
CROSS BORDER DATA TRANSFER MECHANISMS

1. Definitions
   1.1. "*EEA*" means the European Economic Area
   1.2. "*EU Standard Contractual Clauses*" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
   1.3. "*UK International Data Transfer Agreement*" means the International Data Transfer DPA to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.
   2.1. Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in Section 2.3 (EU Standard Contractual Clauses) of this Schedule III; (b) the UK International Data Transfer Agreement as set forth in Section 2.4 (UK International Data Transfer Agreement) of this Schedule III; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Privacy Law.
   2.2. **EU Standard Contractual Clauses**. The EU Standard Contractual Clauses will apply to personal data that is transferred via the Services from the EEA or Switzerland to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, FDPIC) as providing an adequate level of protection for personal data. For data transfers from the EEA that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
      2.2.1. Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Client is a controller of Client Data and Forsta is processing Client Data;
      2.2.2. Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Client is a processor of Client Data and Forsta is processing Client Data;
      2.2.3. Module Four (Processor to Controller) of the Eu Standard Contractual Clauses will apply where Client instructs Forsta to transfer Client Data to Client or its Affiliate incorporated in any country or recipient outside the EEA or Switzerland that is a country not recognized by the European Commission (or, in the case of transfers from Switzerland, FDPIC) as providing an adequate level of protection for personal data.
      2.2.4. For each Module, where applicable:
         2.2.4.1. in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;
         2.2.4.2. in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in this DPA;
         2.2.4.3. in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;
         2.2.4.4. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Norwegian law;
         2.2.4.5. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Norway;
         2.2.4.6. in Annex I, Part A of the EU Standard Contractual Clauses:
            2.2.4.6.1. Data Exporter: Client
            2.2.4.6.2. Contact details: The email address(es) designated by Client in Client's account via its notification preferences.
            2.2.4.6.3. Data Exporter Role: The Data Exporter's role is set forth in this DPA.
            2.2.4.6.4. Signature and Date: By entering into this DPA, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein,

including their Annexes, as of the effective date of the Agreement.

2.2.4.6.5. Data Importer: Forsta

2.2.4.6.6. Contact details: Forsta Privacy Team - privacy@Forsta.com

2.2.4.6.7. Data Importer Role: The Data Importer's role is set forth in this DPA.

2.2.4.6.8. Signature and Date: By entering into this DPA, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;

2.2.4.7. in Annex I, Part B of the EU Standard Contractual Clauses:

2.2.4.7.1. The categories of data subjects are set forth in Section 4 of Schedule I (Details of Processing) of this DPA.

2.2.4.7.2. The Sensitive Data transferred is set forth in Section 6 of Schedule I (Details of Processing) of this DPA.

2.2.4.7.3. The frequency of the transfer is a continuous basis for the duration of the Agreement.

2.2.4.7.4. The nature of the processing is set forth in Section 1 of Schedule I (Details of Processing) of this DPA.

2.2.4.7.5. The purpose of the processing is set forth in Section 1 of Schedule I (Details of Processing) of this DPA.

2.2.4.7.6. The period for which the personal data will be retained is set forth in Section 3 of Schedule I (Details of Processing) of this DPA.

2.2.4.7.7. For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth in Section 7 of Schedule I (Details of Processing) of this DPA.

2.2.4.8. in Annex I, Part C of the EU Standard Contractual Clauses: The Norwegian Data Protection Authority will be the competent supervisory authority; and

2.2.4.9. Schedule II (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

2.3. **UK International Data Transfer Agreement**. The parties agree that the UK International Data Transfer Agreement will apply to personal data that is transferred via the Services from the United Kingdom to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

2.3.1. In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information is located in 2.2.4.6 of this Schedule.

2.3.2. In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.2 (EU Standard Contractual Clauses) of this Schedule III.

2.3.3. In Table 3 of the UK International Data Transfer Agreement:

2.3.3.1. The list of Parties is located in 2.2.4.6 of this Schedule.

2.3.3.2. The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule I (Details of the Processing).

2.3.4. Annex II is located in Schedule II (Technical and Organizational Security Measures).

2.3.5. Annex III, the list of sub-processors, is located at https://legal.forsta.com/legal/forsta-sub-processor-list/.

2.3.6. In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.3.7. Conflict. To the extent there is any conflict or inconsistency between

(a) the EU Standard Contractual Clauses or UK International Data Transfer Agreement; and

(b) any other terms in this DPA (including Schedule IV (Jurisdiction Specific

Terms)), the Agreement, or the Forsta Privacy Notice;
the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.

SCHEDULE IV
JURISDICTION SPECIFIC TERMS

1. Australia:
   1.1. The definition of "Applicable Data Privacy Law" includes the Australian Privacy Principles and the Australian Privacy Act (1988).
   1.2. The definition of "personal data" includes "Personal Information" as defined under Applicable Data Privacy Law.
   1.3. The definition of "Sensitive Data" includes "Sensitive Information" as defined under Applicable Data Privacy Law.
2. Brazil:
   2.1. The definition of "Applicable Data Privacy Law" includes the Lei Geral de Proteção de Dados (LGPD).
   2.2. The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to data subjects.
   2.3. The definition of "processor" includes "operator" as defined under Applicable Data Privacy Law.
3. California:
   3.1. The definition of "Applicable Data Privacy Law" includes the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).
   3.2. The definition of "personal data" includes "Personal Information" as defined under Applicable Data Privacy Law and, for clarity, includes any Personal Information contained within Client Data.
   3.3. The definition of "data subject" includes "Consumer" as defined under Applicable Data Privacy Law. Any obligations related to data subject rights under this DPA, apply equally to Consumers' rights. Regarding Consumer requests per their rights under CCPA and CPRA, Forsta can only verify a request from Client and not from Client's end user or any third party.
   3.4. The definition of "controller" includes "Business" as defined under Applicable Data Privacy Law.
   3.5. The definition of "processor" includes "Service Provider" as defined under Applicable Data Privacy Law.
   3.6. Forsta will process, retain, use, and disclose personal data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Forsta agrees not to (a) sell (as defined by the CCPA and CPRA) Client's personal data or Client end users' personal data; (b) retain, use, or disclose Client's personal data for any commercial purpose (as defined by the CCPA and CPRA) other than providing the Services; or (c) retain, use, or disclose Client's personal data outside of the scope of the Agreement. Forsta understands its obligations under the Applicable Data Privacy Law and will comply with them.
   3.7. Forsta certifies that its sub-processors are Service Providers under Applicable Data Privacy Law, with whom Forsta has entered into a written contract that includes terms substantially similar to this DPA. Forsta conducts appropriate due diligence on its sub-processors.
   3.8. Forsta will implement and maintain reasonable security procedures and practices appropriate to the nature of the personal data it processes as set forth in this DPA.
4. Canada:
   4.1. The definition of "Applicable Data Privacy Law" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
   4.2. Forsta's sub-processors are third parties under Applicable Data Privacy Law, with whom Forsta has entered into a written contract that includes terms substantially similar to this DPA. Forsta has conducted appropriate due diligence on its sub-processors.
   4.3. Forsta will implement technical and organizational measures as set forth in this DPA.
5. European Economic Area (EEA):
   5.1. The definition of "Applicable Data Privacy Law" includes the General Data Protection Regulation (EU 2016/679) ("*GDPR*").
   5.2. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without

limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

6. Israel:
   - 6.1. The definition of "Applicable Data Privacy Law" includes the Protection of Privacy Law (PPL).
   - 6.2. The definition of "controller" includes "Database Owner" as defined under Applicable Data Privacy Law.
   - 6.3. The definition of "processor" includes "Holder" as defined under Applicable Data Privacy Law.
   - 6.4. Forsta will require that any personnel authorized to process Client Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Privacy Law. Such personnel are under confidentiality obligations in accordance with this DPA.
   - 6.5. Forsta must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in this DPA and complying with the terms of the Agreement.
   - 6.6. Forsta must ensure that the personal data will not be transferred to a sub-processor unless such sub-processor has executed an agreement with Forsta pursuant to this DPA.
7. Japan:
   - 7.1. The definition of "Applicable Data Privacy Law" includes the Act on the Protection of Personal Information (APPI).
   - 7.2. The definition of "personal data" includes "Personal Information" as defined under Applicable Data Privacy Law.
   - 7.3. The definition of "controller" includes "Business Operator" as defined under Applicable Data Privacy Law. As a Business Operator, Forsta is responsible for the handling of personal data in its possession.
   - 7.4. The definition of "processor" includes a business operator entrusted by the Business Operator with the handling of personal data in whole or in part (also a "trustee"), as defined under Applicable Data Privacy Law. As a trustee, Forsta will ensure that the use of the entrusted personal data is securely controlled.
8. Mexico:
   - 8.1. The definition of "Applicable Data Privacy Law" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).
   - 8.2. When acting as a processor, Forsta will:
     - 8.2.1. treat personal data in accordance with Client's instructions set forth in this DPA;
     - 8.2.2. process personal data only to the extent necessary to provide the Services;
     - 8.2.3. Implement security measures in accordance with Applicable Data Privacy Law and the security obligations of this DPA;
     - 8.2.4. keep confidentiality regarding the personal data processed in accordance with the Agreement;
     - 8.2.5. delete all personal data upon termination of the Agreement in accordance this DPA; and
     - 8.2.6. only transfer personal data to sub-processors in accordance with this DPA.
9. Singapore:
   - 9.1. The definition of "Applicable Data Privacy Law" includes the Personal Data Protection Act 2012 (PDPA).
   - 9.2. Forsta will process personal data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in this DPA and complying with the terms of the Agreement.
10. Switzerland:
    - 10.1. The definition of "Applicable Data Privacy Law" includes the Swiss Federal Act on Data Protection, as revised (FADP).
    - 10.2. To the extent that personal data transfers from Switzerland are subject to the EU Standard Contractual Clauses in accordance with Section 2.2 of Schedule III (Cross Border Data Transfer Mechanisms), the following amendments will apply to the EU Standard Contractual Clauses:
      - 10.2.1. references to "EU Member State" and "Member State' will be interpreted to include Switzerland, and
      - 10.2.2. insofar as the transfer or onward transfers are subject to the FADP:

10.2.2.1. references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

10.2.2.2. the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

10.2.2.3. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and

10.2.2.4. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

11. United Kingdom (UK):

11.1. References in this DPA to GDPR will be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

11.2. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.