DATA PROCESSING AGREEMENT

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

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

DEFINITIONS

"**Affiliate**" means with respect to a party, any entity controlled by, or under common control with that party. As used in this definition, control means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a party whether through the ownership of voting securities, by contract, or otherwise.

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

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

"**Data Security Standards**" or "DSS" "means the PG Security Exhibit and other information security related provisions contained in the Agreement.

"**Forsta Data**" means (a) any personal data furnished to Vendor by Forsta (or on behalf of Forsta) in relation to using the Services and (b) data stored on Forsta's behalf such as communication logs within the Services or marketing campaign data that Forsta has uploaded to the Services.

"**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.

"**processor**" means the entity which processes personal data on behalf of Forsta; "**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.

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

"**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.

"**Services**" means the products and services provided by Vendor or its Affiliates, as applicable.

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

1. SCOPE OF PROCESSING

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

1.2. **Instructions:** Vendor will only process personal data on documented instructions from Forsta (unless required to do so by a law to which Vendor is subject), contained herein and in written communications between the Parties. In the case of processing required by law, Vendor shall inform Forsta of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

1.3. **Lawfulness of Instruction**: Vendor shall immediately inform Forsta if, in Vendor's opinion, instructions given by Forsta 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. Additional instructions outside the scope of the Agreement or this DPA will be agreed to between the parties in writing.

1.4. **Nature, scope and purpose of the processing**

a) Vendor 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 Forsta. 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"), Vendor warrants that it has provided Forsta use of the necessary additional safeguards that may be required under Applicable Data Privacy Law via Vendor's technical and organizational measures described herein.

b) Vendor shall: (i) not sell or share Forsta's personal Data or Forsta 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; (ii) use Personal Data for the business purpose(s) set forth in the Agreement, and not retain, use, or disclose Personal Data, except where permitted by Applicable Data Privacy Laws, for any purpose other than the business purpose(s) or outside of the direct business relationship between Vendor and Forsta; (iii) notify Forsta if it determines it can no longer meet its obligations under Applicable Data Privacy Laws; (iv) not combine Personal Data, except to the extent permitted by Applicable Data Privacy Laws, with personal information that Vendor receives from, or on behalf of, other persons or with personal information Vendor collects from its own interactions with consumers; (v) by complying with the obligations set out in Section 2 of this DPA, permit Forsta to take reasonable and appropriate steps to ensure Vendor Processes Personal Data in a manner consistent with Forsta's obligations under Applicable Data Privacy Laws; and (vi) work together with Forsta in good faith to remediate any allegedly unauthorized use of Personal Data, if Forsta reasonably believes that Vendor is Processing Personal Data in an unauthorized manner and provides Vendor with reasonable notice of such belief. As used in this Section 1.4, "business," "business purpose," "consumer," "personal information," "sell," and "share," shall have the meanings ascribed to them under Applicable Data Privacy Laws.

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

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

2. COMPLIANCE, INFORMATION DISTRIBUTION, AUDITS

2.1. Vendor will maintain the certifications and attestations stated in the Data Security Standards.

2.2. **Assistance:** Vendor will provide reasonable additional and timely assistance to assist Forsta in complying with its data protection obligations in connection with Vendor's processing of Forsta Data (including Personal Data) and with respect to data subject rights and Controller under Applicable Data Privacy Law. Forsta may share this DPA with relevant controllers of Forsta Data if required, redacting to protect business secrets/confidential information, if any. Vendor will reasonably assist Forsta with its obligation to 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 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.

2.3. **Data Subject Rights**: Vendor will provide Forsta with the ability to access, correct, rectify, erase, or block Personal Data, or to transfer or port such Personal Data, within the Services, as may be required under Applicable Data Privacy Laws (collectively, "Data Subject Requests"). Notwithstanding, 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 Forsta 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.

2.4. **Audit.** Vendor will audit its compliance with its security obligations hereunder using industry standard methods and may use a third party to do so. Vendor will perform such audits at least once annually at Vendor's expense to result in the generation of a confidential audit report ("Audit Report"). Subject to reasonable confidentiality controls, Vendor will make available to Forsta a copy of Vendor's most recent Audit Report. Vendor will allow for and contribute to audits. Forsta may audit Vendor's compliance with its obligations in this DPA and relevant Data Security Standards.

3. SECURITY, CONFIDENTIALITY, BREACH NOTIFICATION

3.1. Vendor will maintain appropriate technical and organizational safeguards to protect the security, confidentiality, and integrity of Forsta Data, including any Personal Data contained therein, as set forth in the DSS This includes protecting the personal data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the personal data.

3.2. Persons authorized by Vendor to Process Personal Data will be bound by appropriate confidentiality obligations at least as protective as the obligations of Vendor herein. Vendor 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 Forsta. Vendor shall grant access to Forsta Data to its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the contract.

3.3. **Security Incident notification**. Vendor will, notify Forsta of a Security Incident via email to the email address(es) designated by Forsta in Forsta's account, without undue delay, but in every case within 72 hours, after Vendor having become aware of a Security Incident impacting Forsta Data of which Vendor is a processor; and such notification of a Security Incident will contain, at least: a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned); b) the details of a contact point where more information concerning the Security Incident can be obtained; c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

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

4. SUB-PROCESSORS

4.1. **General Authorization**: Forsta authorizes Vendor to engage sub-processors generally, conditioned on the following requirements: a) Vendor will restrict the onward sub-processor's access to Forsta Data only to what is strictly necessary for the purposes listed in Schedule I and will prohibit the sub-processor from processing the personal data for any other purpose; b) Vendor 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 Forsta Data to the standard required by Applicable Data Privacy Law, including the requirements set forth in Schedule III (Jurisdiction Specific Terms) of this DPA, which may include adequate transfer mechanisms, if required; c) Vendor will remain liable for any breach of this DPA that is caused by an act, error, or omission of its sub-processors.

4.2. **Current Sub-processors and Notification of Sub-processor Changes**: If Vendor engages subprocessors, Vendor will maintain an up-to-date list of its sub-processor as detailed in the Agreement and give Forsta written notice of any change to this list 30 days prior to any change

4.3. **Objection Right for new Sub-processors**: Forsta may object to Vendor's appointment or replacement of a sub-processor prior to its appointment or replacement. 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, Forsta shall, without penalty (notwithstanding any term in the Agreement), upon written notice, terminate the Agreement. Such termination will be without prejudice to any fees incurred by Forsta prior to the termination. Vendor shall within 30 days of Forsta's notice of termination, refund to Forsta all pre-paid fees. If no objection has been raised prior to Vendor replacing or appointing a new sub-processor, Forsta will be deemed to have authorized the new sub-processor

5. INTERNATIONAL DATA TRANSFERS

5.1. **Jurisdiction Specific Terms**. To the extent Vendor processes personal data originating from and protected by Applicable Data Privacy Law in one of the jurisdictions listed in Schedule III (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

5.2. **Transfer Mechanism**. To the extent Forsta's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area ("EEA"), the United Kingdom, Switzerland, or any other jurisdiction listed in Schedule III (Jurisdiction Specific Terms) of this DPA) to Vendor located outside of the EEA which is not subject to an adequacy decision (a "*Data Transfer*"); such Data Transfer will be subject to the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as annexed to Commission Implementing Decision 2021/914 ("*SCCs*"), which are incorporated into this DPA by this reference, ("Transfer Mechanism")

5.3. **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 ("SCCs) ; (b) the UK International Data Transfer Agreement ("UK IDTA"); and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Privacy Law.

5.4. **Application of SCCs**.

5.4.1 Modules Module Two (Data Controller to Data Processor) will apply to a Data Transfer when Customer is a Data Controller. Module Three (Data Processor to Data Processor) will apply to a Data Transfer when

Customer is a Data Processor.

5.4.2 Optional provisions. Where the SCCs identify optional provisions:

(a) in Clause 7 (Docking Clause) – the optional provision applies;

(b) in Clause 9(a) (Use of sub-processors) – Option 2 applies (and the parties will follow the process and timings agreed in the DPA to appoint sub-processors);

(c) in Clause 11(a) (Redress) – the optional provision does not apply;

(d) in Clause 17 (Governing law) – option 1 applies, and where the Agreement is governed by the laws of an EU Member State, the laws of that EU Member State apply; otherwise, Norwegian law applies; and

(e) in Clause 18(b) (Choice of forum and jurisdiction) – where the Agreement is subject to the jurisdiction of the courts of an EU Member State, the courts of that EU Member State have jurisdiction; otherwise, the courts of Norway have jurisdiction.

5.4.3 Annexes of SCCs.

(a) In Annex 1A: the data exporter(s) is Forsta and its Affiliates making the Data Transfer (the "Data Exporter") and the data importers are the Vendor entities receiving the Data Transfer (the "Data Importer"). The full name, address and contact details for the Data Exporter and the Data Importer are set out in the Agreement or can be requested by either party.

(b) In Annex 1B: The: relevant details are those set out in the Agreement, including Schedule 1 "Details of Processing" in this DPA.

(c) In Annex 1C: The competent supervisory authority is the supervisory authority applicable to Forsta (or, where relevant, applicable to Forsta's representative).

(d) In Annex 2: the security provisions are those set out in Schedule II "Security Measure" in this DPA.

5.5. **Transfers subject To Swiss Data Protection Law:** If there is a Data Transfer subject to Data Protection Laws of Switzerland, then the SCCs will apply with the following modifications: the competent supervisory authority in Annex 1.C under Clause 13 will be "*the Federal Data Protection and Information Commissioner*"; references to a "*Member State*" and "*EU Member State*" will not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and references to "GDPR" in the SCCs will be understood as references to Data Protection Laws of Switzerland.

5.6. **Transfers subject to UK Data Protection Law**: If there is a Data Transfer subject to Data Protection Laws of the United Kingdom, then the International Data Transfer Agreement (UK IDTA) or International Data Transfer Addendum to the SCCs ("Addendum"), as issued by the Information Commissioner in the United Kingdom will apply and is incorporated by reference into this DPA. The information needed to complete the Tables to the UK IDTA or Addendum is set out in the Agreement, including Schedule 1 "Details of Processing" of this DPA.

5.7. **Execution**. The parties agree that its respective execution of the Agreement is deemed to constitute its execution of the SCCs, the UK IDTA and/or the Addendum on behalf of the Data Exporter/Data Importer (as applicable)

6. MISCELLANEOUS

6.1. **Third Party Beneficiary for Deletion Purposes**. If Forsta has factually disappeared, ceased to exist in law, or has become insolvent, the controller or super-processor (i.e., the processor that instructs Forsta's processing of Forsta Data) shall have the right hereunder to terminate this DPA and to instruct Vendor to erase or return the personal data under its control in accordance with Applicable Data Privacy Law.

6.2. **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 III (Jurisdiction Specific Terms) of this DPA; (2) the terms of this DPA outside of Schedule III (Jurisdiction Specific Terms); and (3) the Agreement. 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.

6.3. **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 in the event of but not limited to (a) changes in Applicable Data Privacy Law; (b) a merger, acquisition, or other similar transaction involving Forsta; or (c) the purchase of new products or services or material changes to any of the existing Services.

SCHEDULE I: DETAILS OF PROCESSING

1. **Nature and Purpose of the Processing**. Vendor will process personal data and Forsta Data as necessary to provide the Services under the Agreement and in accordance with Forsta's instructions as set forth in this DPA.
2. **Duration of the Processing**. The period for which personal data will be retained and the criteria used to determine that period is as follows: a) prior to the termination of the Agreement, Vendor will delete Forsta Data when Forsta elects to delete such Forsta Data; b) upon termination of the Agreement, Vendor shall automatically delete any stored Forsta Data (including Forsta Data on Vendor's back-up systems) thirty (30) days after the termination effective date;. Any Forsta Data archived on Vendor's back-up systems shall be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.
3. **Categories of Data Subjects**: The categories of data subjects are determined by Forsta throughout the term of the Agreement but may include Forsta's clients, customers, employees, suppliers, agents, partners and/or end users.
4. **Types of Personal Data**: The categories of personal data are determined by Forsta throughout the term of the Agreement but may include any Personal Data included in Forsta Data which is uploaded to the Services.
5. **Sensitive Data or Special Categories of Data**. Forsta or its end users may choose to include Sensitive Data within data that is collected via the Services.
6. **Sub-Processors:** if applicable, Vendor's Subprocessors' list as approved by Forsta is incorporated by referenced. The subject matter, nature, and duration of the processing carried out by Vendor's sub-processors are the same as those by Vendor itself.

SCHEDULE II: SECURITY MEASURES

1.1. The security provisions contained in the Data Security Standards and other information security related provisions in the Agreement will apply to the Vendor and any subprocessor engaged by the Vendor.

1.2. When Vendor engages a sub-processor under this DPA, Vendor and the sub-processor will enter into an agreement with data protection obligations substantially similar to those contained in this DPA. Each sub-processor agreement must ensure that Vendor is able to meet its obligations to Forsta. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify Vendor in the event of a Security Incident so Vendor may notify Forsta; (b) delete personal data when instructed by Vendor in accordance with Forsta's instructions to Vendor; (c) not engage additional sub-processors without Vendor'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 Forsta's instructions to Vendor.

SCHEDULE III: JURISDICTION SPECIFIC TERMS

1. **Australia:** The definition of "Applicable Data Privacy Law" includes the Australian Privacy Principles and the Australian Privacy Act (1988); "personal data" includes "Personal Information" as defined under Applicable Data Privacy Law; "Sensitive Data" includes "Sensitive Information" as defined under Applicable Data Privacy Law.
2. **Brazil:** The definition of "Applicable Data Privacy Law" includes the Lei Geral de Proteção de Dados (LGPD); "Security Incident" includes a security incident that may result in any relevant risk or damage to data subjects; "processor" includes "*operator*" as defined under Applicable Data Privacy Law.
3. **California:** The definition of "*Applicable Data Privacy Law*" includes the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA); "*personal data*" includes "*Personal Information*" as defined under Applicable Data Privacy Law and, for clarity, includes any Personal Information contained within Forsta Data; "*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, Vendor can only verify a request from Forsta and not from Forsta's end user or any third party; "*controller*" includes "*Business*" as defined under Applicable Data Privacy Law; "processor" includes "Service Provider" as defined under Applicable Data Privacy Law. Vendor will process, retain, use, and disclose personal data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Vendor agrees not to (a) sell (as defined by Applicable Data Privacy Law) Forsta's personal data or Forsta end users' personal data; (b) retain, use, or disclose Forsta's personal data for any commercial purpose (as defined by Applicable Data Privacy Law) other than providing the Services; or (c) retain, use, or disclose Forsta's personal data outside of the scope of the Agreement. Vendor understands its obligations under the Applicable Data Privacy Law and will comply with them. Vendor certifies that its sub-processors are Service Providers under Applicable Data Privacy Law, with whom Vendor has entered into a written contract that includes terms substantially similar to this DPA. Vendor conducts appropriate due diligence on its sub-processors. Vendor 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**: The definition of "*Applicable Data Privacy Law*" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA). Vendor's sub-processors are third parties under Applicable Data Privacy Law, with whom Vendor has entered into a written contract that includes terms substantially similar to this DPA. Vendor has conducted appropriate due diligence on its sub-processors and shall implement technical and organizational measures as set forth in this DPA.
5. **European Economic Area (EEA)**: The definition of "*Applicable Data Privacy Law*" includes the General Data Protection Regulation (EU 2016/679) ("*GDPR*"). 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:** The definition of "*Applicable Data Privacy Law*" includes the Protection of Privacy Law (PPL); "*controller*" includes "Database Owner" and "processor" includes "Holder" as defined under Applicable Data Privacy Law. Vendor shall require that any personnel authorized to process Forsta 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. Vendor 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. Vendor must ensure that the personal data will not be transferred to a sub-processor unless such sub-processor has executed an agreement with Vendor pursuant to this DPA.

7. **Japan:** The definition of "*Applicable Data Privacy Law*" includes the Act on the Protection of Personal Information (APPI); "*personal data*" includes "*Personal Information*"; "*controller*" includes "*Business Operator*" as defined under Applicable Data Privacy Law. As a Business Operator, Vendor is responsible for the handling of personal data in its possession; 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, Vendor will ensure that the use of the entrusted personal data is securely controlled.
8. **Mexico:** 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). When acting as a processor, Vendor will: a) treat personal data in accordance with Forsta's instructions set forth in this DPA; b) process personal data only to the extent necessary to provide the Services; c) implement security measures in accordance with Applicable Data Privacy Law and the security obligations of this DPA; d) keep confidentiality regarding the personal data processed in accordance with the Agreement; e) delete all personal data upon termination of the Agreement in accordance this DPA; and f) only transfer personal data to sub-processors in accordance with this DPA.
9. **Singapore:** The definition of "*Applicable Data Privacy Law*" includes the Personal Data Protection Act 2012 (PDPA). Vendor 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**: The definition of "*Applicable Data Privacy Law*" includes the Swiss Federal Act on Data Protection, as revised (FADP). To the extent that personal data transfers from Switzerland are subject to a Transfer Mechanism, the following amendments will apply to the EU Standard Contractual Clauses: a) references to "EU Member State" and "Member State' will be interpreted to include Switzerland, and b) insofar as the transfer or onward transfers are subject to the FADP, references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP; the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner; in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.
11. **United Kingdom (UK):** 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). 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.