DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into accessiBe's Terms of Service at https://accessibe.com/terms-of-service or other agreement governing the use of accessiBe's services ("**Agreement**") entered by and between you, the Customer or Partner (as such terms are defined in the Agreement) (collectively, "**you**", "**your**", "**Customer**"), and accessiBe Ltd. or an Affiliate thereof ("**accessiBe**"; the term "accessiBe" shall refer to accessiBe Ltd. and its Affiliates, as applicable) to reflect the Parties' agreement with regard to the Processing of Personal Data by accessiBe solely on behalf of the Customer. Each of the parties hereto may also be referred to as a "**Party**", and together as the "**Parties**".

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement. In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. DEFINITIONS

1.1 Definitions:

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which is explicitly permitted to use the Services under the Agreement but has not signed its own agreement with accessiBe and is not a "Customer" or "Partner" under the Agreement.

(c) The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CPRA.

(d) For clarity, within this DPA, "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent that the CPRA applies. In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider.

(e) "**Data Protection Laws**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**"), the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and California Privacy Rights Act of 2020 (the "**CPRA**").

(f) "**Data Subject**" means an identified or identifiable natural person; 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Data Subject includes Consumer as such term is defined under the CPRA.

(g) "**EU Standard Contractual Clauses**" or "**EU SCCs**" shall mean the Standard Contractual Clauses set out in the Annex of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(h) "**Personal Data**" means any information relating to a Data Subject. Personal Data includes Personal Information as such term is defined under the CPRA.

(i) "**Restricted Transfer**" means a transfer (directly or via onward transfer) of Personal Data that is subject to the GDPR, the UK GDPR or Swiss data protection laws to a country outside of the European Economic Area, the United Kingdom or Switzerland that is not subject to an adequacy decision by the European Commission, or the competent UK or Swiss authorities (as applicable).

(j) "**Services**" means the services provided to Customer by accessiBe in accordance with the Agreement.

(k) "**Security Documentation**" means the security documentation applicable to the Services purchased by Customer, as updated from time to time, and made reasonably available by accessiBe upon Customer's request.

(l) "**Sensitive Data**" means Personal Data that is protected under special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Laws.

(m) "**Sub-processor**" means any third party that Processes Personal Data under the instruction or supervision of accessiBe.

(n) "**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office in the UK (available under:

https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf)

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. This DPA applies when Personal Data is Processed by accessiBe as part of accessiBe's provision of the Service, as further specified in the Agreement and any applicable order form. The Parties acknowledge and agree that with regard to the Processing of Personal Data on behalf of Customer that is subject to the GDPR, the UK GDPR, or the CPRA, (i) Customer is the Controller or Business, respectively, and (ii) accessiBe is the Processor or Service Provider, respectively.

2.2 **Customer's Responsibilities**. Customer undertakes to provide all necessary notices to Data Subject and receive all necessary permissions and consents, or otherwise secure the required legal bases in order to collect, Process, and transfer to accessiBe the Personal Data, and as necessary for accessiBe's Processing activities on Customer's behalf under the terms of the Agreement and this DPA, pursuant to the applicable Data Protection Laws. To the extent required under applicable Data Protection Laws, Customer will appropriately

document the Data Subjects' notices and consents, or necessary assessment with other applicable lawful grounds of Processing.

2.3 **accessiBe's Processing of Personal Data**. When Processing on Customer's behalf under or as required by the Agreement, accessiBe shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and as part of its provision of the Services; (ii) Processing to comply with Customer's other reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed; (iii) rendering Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder.

2.4 Notwithstanding, Personal Data may be disclosed by accessiBe (a) if required by a subpoena or other judicial or administrative order, or if otherwise required by law; or (b) if accessiBe deems the disclosure necessary to protect the safety and rights of any person, or the general public.

2.5 accessiBe shall inform Customer without undue delay if, in accessiBe's opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Laws. To the extent that accessiBe cannot comply with an instruction from Customer, (i) accessiBe shall inform Customer, providing relevant details of the issue, (ii) accessiBe may, without liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) or suspend Customer's access to the Services, and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to accessiBe all the amounts owed to accessiBe or due before the date of termination. Customer will have no further claims against accessiBe (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.6 **Details of the Processing**. The subject matter of Processing of Personal Data by accessiBe 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 Schedule 1 (Details of Processing) to this DPA.

2.7 **Sensitive Data**. The Parties agree that the Services are not intended for the processing of Sensitive Data, and that if Customer wishes to use the Services to process Sensitive Data, it must first obtain accessiBe's explicit prior written consent and enter into any additional agreements as required by accessiBe.

2.8 **CPRA Standard of Care; No Sale of Personal Information**. accessiBe will not (1) sell (as defined in the CPRA or other Data Protection Laws) Personal Data, or (2) retain, use or disclose Personal Data: (i) for any purpose other than for the specific purpose of performing the Subscription Services, (ii) outside of the direct business relationship between Customer and accessiBe, except as permitted under applicable Data Protection Laws, or (3) combine Personal Data received pursuant to the Agreement with personal information (as defined in the CPRA) (i) received from or on behalf of another person, or (ii) collected from accessiBe's own interaction with any Data Subject to whom such Personal Data pertains. accessiBe

does not receive any Personal Data from Customer as consideration for its provision of the Subscription Services. accessiBe certifies that it understands the restrictions set forth in this Section and will comply with them.

3. DATA SUBJECT REQUESTS

accessiBe shall, to the extent legally permitted, notify Customer or refer Data Subject or Consumer to Customer, if accessiBe receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under applicable Data Protection Laws) of access, right to rectification, restriction of Processing, erasure, data portability, objection to the Processing, their right not to be subject to automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against ("**Data Subject Request**"). Considering the nature of the Processing, accessiBe shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. accessiBe may advise Data Subjects on available features for self-exercising their Data Subject Requests through the Services (where appropriate), or refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. CONFIDENTIALITY

accessiBe shall ensure that its personnel and advisors engaged in the Processing of Personal Data (i) are contractually bound to confidentiality requirements no less than what is required under this DPA and (ii) are informed of the confidential nature of Personal Data and required to keep it confidential.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors**. Customer acknowledges and agrees that (a) any accessiBe Affiliate may be engaged as a Sub-processor; and (b) accessiBe and an accessiBe Affiliate on behalf of accessiBe may each engage third-party Sub-processors in connection with the provision of the Services. A list of Sub-processors is available upon request at legalnotices@accessibe.com.

5.2 **List of Current Sub-processors and Notification of New Sub-processors**.

Customer hereby provides accessiBe with a general authorization to engage the Sub-processors. All Sub-processors have entered into written agreements with accessiBe that bind them by substantially the same material data protection obligations under this DPA.

5.3 **Objection to New Sub-processors**. accessiBe shall provide Customer with notification of any intended new Sub-processor(s) by sending an e-mail to the email address provided by Customer to accessiBe (including through the Customer's dashboard/portal on accessiBe's website). Customer may reasonably object to accessiBe's use of a new Sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by notifying accessiBe promptly in writing within seven (7) days after receiving the above notice. Such written objection shall include the reasons for objecting to accessiBe's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within seven (7) days following accessiBe's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new

Sub-processor, as permitted in the preceding sentences, accessiBe will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If accessiBe is unable to make available such change within thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Processor without the use of the objected-to new Sub-processor, by providing written notice to accessiBe. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to accessiBe. Until a decision is made regarding the new Sub-processor, accessiBe may temporarily suspend the Processing of the affected Personal Data or suspend access to the Account. Customer will have no further claims against accessiBe due to the termination of the Agreement (including, without limitation, requesting refunds) or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors**. Where accessiBe engages a Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular obligations to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR. Where a Sub-processor fails to fulfil its data protection obligations concerning its Processing of Personal Data, accessiBe shall remain responsible for the performance of the Sub-processor's obligations.

6. SECURITY & AUDITS

6.1 **Controls for the Protection of Personal Data**. accessiBe shall maintain industry-standard technical and organizational measures for protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data, including those measures set forth in the Security Documentation), as may be amended from time to time. Detailed information regarding such safeguards is set forth in Annex II of the Standard Contractual Clauses, as attached hereto as Schedule 2. Upon the Customer's reasonable request, accessiBe will reasonably assist Customer, at Customer's cost and subject to the provisions of Section 11.1 below, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and the information available to accessiBe.

6.2 **Audits and Inspections**. Upon Customer's 30 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer, accessiBe shall make available to Customer (or Customer's independent, reputable, third-party auditor that is not a competitor of accessiBe and not in conflict with accessiBe, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them, provided that such auditor will not have access to non-Customer data. accessiBe may satisfy the audit obligation under this section by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors. Any information, audits,

inspections and the results from such audits, including the documents reflecting the outcome of the audit or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without accessiBe's prior written approval. Upon accessiBe's first request, Customer shall return or permanently destroy all records or documentation in Customer's possession or control provided by accessiBe in the context of the audit or the inspection. If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 6.2 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

6.3 In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to accessiBe's premises, equipment, personnel and business while conducting such audit or inspection.

6.4 The audit rights set forth in 6.2 above, shall only apply to the extent that the Agreement does not otherwise provide Customer with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

accessiBe maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by accessiBe on behalf of the Customer (a "**Data Incident**"). accessiBe's notice will at least: (a) describe the nature of the Data Incident including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) communicate the name and contact details of accessiBe's data protection team, which will be available to provide any additional Data Incident; (c) describe the measures taken or proposed to be taken by accessiBe to address the Data Incident, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Data Incident which directly or indirectly identifies accessiBe (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without accessiBe's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Customer shall provide accessiBe with reasonable prior written notice to provide accessiBe with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required.

8. RETURN AND DELETION OF PERSONAL DATA

Within 90 days following termination of the Agreement and subject thereto, accessiBe shall, at the choice of Customer (indicated through the Services or in written notification to accessiBe), delete or return to Customer all the Personal Data it Processes solely on behalf

of the Customer in the manner described in the Agreement, and accessiBe shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, accessiBe may also retain one copy of the Personal Data as necessary in connection with its routine backup and archiving procedures for evidence purposes or for the establishment, exercise or defense of legal claims or for compliance with legal obligations under applicable law.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level or data protection**. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), Switzerland and the United Kingdom ("**UK**") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, Switzerland, or the UK as relevant, as applicable, without any further safeguard being necessary.

9.2 accessiBe participates in and certifies compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework (together, the "**Data Privacy Framework**"). accessiBe will (i) provide at least the same level of privacy protection as required by the Data Privacy Framework Principles; (ii) notify Customer if accessiBe makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) upon notice, including under the preceding sub-section (ii), take reasonable and appropriate steps to remediate unauthorized processing.

9.3 If accessiBe transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, accessiBe will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws and Regulations.

9.4 As applicable, if: (i) the Data Privacy Framework is invalidated; (ii) accessiBe is no longer able to continue complying with the principles of the Data Privacy Framework; (iii) an adequacy recognition is invalidated or otherwise terminated, then a transfer of Personal Data outside of the EEA, the UK or Switzerland to accessiBe shall constitute a Restricted Transfer and Section 9.5 shall apply.

9.5 The parties agree that when the transfer of personal data from Customer to accessiBe is a Restricted Transfer, such Restricted Transfer will be subject to the clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"), which are deemed incorporated and for a part of this DPA as follows:

9.5.1 In relation to Restricted Transfers of Customer's Personal Data protected by the GDPR, the EU SCCs will apply, completed as follows:

(i) the module specified in **Schedule 2** will apply;

(ii) In Clause 7, the optional docking clause will apply.

(iii) In Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be as set out in Section 5 of this DPA.

(iv) In Clause 11, the optional language will not apply.

(v) In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law.

(vi) In clause 18(b), disputes will be resolved before the courts of Ireland.

9.5.2 accessiBe will implement and maintain the technical measures, as specified in Annex II of Exhibit A, which is attached and incorporated by reference to this DPA, with a purpose to protect the EEA Transferred Data from Processing for national security or other governmental purposes that goes beyond what is necessary and proportionate in a democratic society, considering the type of Processing activities under the Agreement and relevant circumstances;

9.5.3 In order to safeguarding EEA Transferred Data, when any government or regulatory agency of a Third Country ("**Authority**") requests access to such data ("**Request**"), and unless required by a valid court order or if otherwise accessiBe may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to EEA Transferred Data, or where the access is requested in the event of imminent threat to lives, accessiBe will:

(i) not allow access to EEA Transferred Data, for example by providing any Authority with encryption keys; and

(ii) upon Customer's written request, provide reasonable available information about the requests of access to Personal Data by government agencies that accessiBe has received in the six (6) months preceding to Customer's request.

9.5.4 If accessiBe receives a Request, accessiBe will notify Customer of such request to enable the Customer to take necessary actions, to communicate directly with the relevant agency and to respond to the Request. If accessiBe is prohibited by law to notify the Customer of the Request, accessiBe will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer's expense and, to the extent possible, will provide only the minimum amount of information necessary.

9.5.5 In relation to transfers of UK GDPR-governed Personal Data ("**UK Transferred Data**") to a Third Country, the EU SCCs: (i) apply as completed in accordance with sections 9.2 and 9.3 above; and (ii) are deemed amended as specified by the UK Addendum, which is deemed executed by the parties and incorporated into and forming an integral part of this DPA.

9.5.6 In addition, Tables 1 to 3 in Part 1 of the UK Addendum is deemed completed respectively with the information in Annex I and II of Exhibit A; Table 4 in Part 1 is deemed completed by selecting "neither party." Any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

9.5.7 In relation to Restricted Transfers of Customer's Personal Data that is subject to the Swiss FDPA ("**Swiss Transferred Data**"), the following modifications shall apply to the EU SCCs to the extent that the Swiss FDPA applies to accessiBe's Processing of Customer's Personal Data: (a) the term "member state" as used in the EU SCCs will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; (b) references to the GDPR or other governing law contained in the EU SCCs shall also be interpreted to include the Swiss FDPA; and (c) the parties agree that the supervisory authority as indicated in Annex I.C of the EU SCCs shall be the Swiss Federal Data Protection and Information Commissioner.

9.5.8 The terms set forth in Part 2 of **Schedule 2** (Additional Safeguards) shall apply to an EEA Transfer and a UK Transfer.

10. AUTHORIZED AFFILIATES

10.1 **Contractual Relationship**. The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate shall be deemed to have agreed to be bound by the Customer's obligations under this DPA, if and to the extent that accessiBe Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "**Controller**". All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA, and the Customer shall procure that each Authorized Affiliate so complies, and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

10.2 **Communication**. Customer shall remain responsible for coordinating all communication with accessiBe under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11. OTHER PROVISIONS

11.1 **Data Protection Impact Assessment and Prior Consultation**. Upon Customer's reasonable request, accessiBe shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR or the UK GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to accessiBe. accessiBe shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 12.1, to the extent required under the GDPR or the UK GDPR, as applicable.

11.2 **Modifications**. Each Party may by at least forty-five (45) calendar days' prior written notice to the other Party, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Customer Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. Pursuant to such notice: (a) The Parties shall

make commercially reasonable efforts to accommodate such modification requested by Customer or that accessiBe believes is necessary; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by accessiBe to protect accessiBe against additional risks, or to indemnify and compensate accessiBe for any further steps and costs associated with the variations made herein at Customer's request. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's or accessiBe's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then Customer or accessiBe may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof). Customer will have no further claims against accessiBe (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Agreement and the DPA as described in this Section.

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Services to Customer;
2. Performing the Agreement, this DPA other contracts executed by the Parties;
3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;
4. Sharing Personal Data with third parties in accordance with Customer's instructions or pursuant to Customer's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Customer to facilitate the sharing of Personal Data between the Services and such third party services);
5. Complying with applicable laws and regulations;
6. All tasks related to any of the above.

Duration of Processing

Subject to any section of the DPA or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, accessiBe will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

The Personal Data processed depends on the types of Personal Data provided by the Customer and may include name, email address, and telephone number.
End-Users' IP address and URL.
The customer shall not submit any Sensitive Data unless explicitly agreed by accessiBe.

Categories of Data Subjects

Customer's employees, Customer's customers/clients, Customer's End-Users (to the extent Personal Data is provided in the context of the Services rendered).

SCHEDULE 2

ANNEX to the COMMISSION IMPLEMENTING DECISION on 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 officially published at: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf or other official publications of the European Union as updated from time to time:

MODULE TWO: Transfer controller to processor; or

MODULE THREE: Transfer processor to processor

ANNEX I

Details of Processing

PART 1

If the EU or UK Standard Contractual Clauses apply, the data exporter(s) and importer(s) are identified as follows:
Data Exporter: Customer.

Contact details: As detailed in the Agreement.

Data Exporter Role:

Module Two: The Data Exporter is a data controller.

Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: accessiBe.

Contact details: As detailed in the Agreement.

Data Importer Role:

Module Two: The Data Importer is a data processor.

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

1. **Description of the Transfer**:

   The categories of data subjects are described in Schedule 1 (Details of Processing) of this DPA.

   The categories of personal data are described in Schedule 1 (Details of Processing) of this DPA.

   The Parties do not intend for Sensitive Data to be transferred.

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

   The nature of the processing is described in Schedule 1 (Details of Processing) of this DPA.

   The purpose of the processing is described in Schedule 1 (Details of Processing) of this DPA.

   The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement or the DPA.

   In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth in the list of Sub-processors pursuant to Section 5.2 of the DPA.

2. **Annex II - Technical and organizational security measures**

accessiBe maintains regularly updating policies and procedures, to uphold high standards and appropriate technical and organizational security measures, including:

- *Data Minimization and Limited Retention*. accessiBe limits data storage to what is necessary for the needs of its customers and required under applicable law.
- *Security Management*. accessiBe maintains a written information security management, including policies, processes, enforcement, and controls governing all data processing, designed to secure Data against accidental or unlawful loss, access or disclosure; identify reasonably foreseeable and internal risks and authorized access; and minimize security risks, including through risk assessment and regular testing.
- *Encryption*. All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.
- *Incident Management*. accessiBe has implemented and maintains an incident response plan and is prepared to respond immediately to a system breach.
- *Physical Access Controls*. Physical controls are used to prevent unauthorized entrance at the perimeter and at building access points. Passage requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.).
- *Logs Management. accessiBe regularly keeps logs of each relevant systems, to ensure their security and reliability*.
- *Security Monitoring*. accessiBe monitors and logs security events for security exceptions and inappropriate user activities on a regular basis and implements automated alerts to identify and respond to security issues.
- Personnel is through a formal security awareness program upon hire and annually.
- Third-Party Vendors. accessiBe conducts due diligence on third-party vendors and requires them to adhere to strict security standards and audits them if it is deemed necessary by authorized personnel.
- Strict Password Policy and Multi-Factor Authentication. accessiBe holds a strict Password Policy, obliging personnel to maintain a multi-character complex password. In addition, multi-factor authentication is implemented for personnel who access sensitive data or systems.
- Access Control. Access to the company information resources is granted for business purposes that are authorized by the relevant management and on need-to-know access.

3. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

PART 2 – Additional Safeguards

1. In the event of an EEA Transfer or a UK Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:

    a. accessiBe shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Customer to accessiBe and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.

    b. If accessiBe becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

        I. accessiBe shall inform the relevant government authority that accessiBe is a processor of the Personal Data and that the Customer has not authorized accessiBe to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon the Customer in writing;

        II. accessiBe will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under accessiBe's control. Notwithstanding the above, (a) the Customer acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, accessiBe has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (e)(II) shall not apply. In such event, accessiBe shall notify the Customer, as soon as possible, following the access by the government authority, and provide the Customer with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, accessiBe will inform the Customer, at the Customer's written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.