

**Data Processing Agreement**  
**Passage Technology, LLC as the Controller**  
*(Revision March 2019)*

This Data Processing Agreement (“DPA”) is made by and between Passage Technology, LLC, an Illinois limited liability company (“Passage”), and Company (the “Company,” and together with Passage, the “Parties,” and each, a “Party”) as of February 18th, 2019 and shall govern any services provided to Passage and its Affiliates by Company as a Processor or Subprocessor (as defined below) (the “Services”). This DPA supplements, is incorporated into, and will remain in effect for the entire term of any agreement (the “Agreement”) between the Parties, including without limitation any written, electronic, and implied executed agreement and, when applicable, Passage’s Terms of Use. This DPA shall remain in effect until termination of the Agreement, the duration of Services, or the deletion of Passage Data, whichever occurs later (the “Term”).

Company undertakes to use a commercially reasonable selection process by which it evaluates the security, privacy, and confidentiality practices of proposed Subprocessors that will or may have access to or process Personal Data (defined below). Passage requires its Processors and Subprocessors to satisfy equivalent obligations as those required of Passage the Company under applicable data protection laws and regulations, including but not limited to the following requirements: (1) process personal data in accordance with data controller’s documented instructions; (2) implement and maintain appropriate technical and organizational measures and to protect against unauthorized access and anticipated threats or hazards to personal data; (3) promptly notify Passage about any actual or potential security breach affecting Personal Data processed on behalf of Passage; and (4) cooperate with Passage in responding to requests from data controllers, data subjects, or data protection authorities, as applicable.

This DPA shall not replace any comparable or additional rights relating to Processing of Personal Data contained in the Agreement.

**1. Definitions.**

References in this DPA to “Controller,” “Data Subject,” “Processor,” and “Supervisory Authority” shall have the meanings ascribed to them under Applicable Privacy Laws. Capitalized terms not defined in this DPA shall have the meaning set out in the Agreement.

“**Affiliate**” means any entity in which the party owns, either directly or indirectly, more than 50% of the equity interest or voting stock, or equivalent, in such entity, or controls, is controlled by or under common control with such entity, whether such entity is now existing or subsequently created or acquired during the term of the DPA.

“**Applicable Privacy Laws**” means all applicable privacy and data protection laws and regulations anywhere in the world, including, where applicable, the EU Data Protection Directive 95/46/EC, the EU Directive 2002/58/EC on privacy and electronic communications, and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (in all cases, as amended, superseded or replaced).

“**Controller**” means the natural or legal person or entity who determines the purposes and means of the processing of Personal Data.

**"Data Breach"** means a breach of security leading to accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and all other unlawful forms of processing of Passage Data.

**"Data Subject"** means the individual to whom Personal Data relates.

**"GDPR"** means the General Data Protection 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.

**"Passage Data"** means any and all data including Personal Data that is provided to Company or otherwise collected and/or accessed by Company on behalf of Passage and/or its Affiliates in the course of providing the Services under the Agreement. Any Passage Data that is Personal Data is hereby referred to as "Passage Personal Data".

**"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

**"Process"** means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

**"Processor"** means an entity that processes Personal Data on behalf of, and in accordance with the instructions of, a Controller.

**"SCCs"** means the standard contractual clauses set forth in Schedule 1 herein.

**"Subprocessor"** means an entity engaged by a Processor who agrees to receive from the Processor Personal Data exclusively intended for the processing activities to be carried out as part of the Services.

## **2. Role of the Parties.**

The Parties acknowledge and agree that with regard to the processing of Personal Data, Passage may be a Controller or a Processor, Company may be a Processor or Subprocessor, and therefore acknowledges that it may act as a Processor of Passage or a Subprocessor of Passage. Where Company acts as a Processor, Passage is obligated contractually and/or under Applicable Privacy Laws to flow down certain data protection related obligations to its appointed Subprocessors. Therefore, all obligations placed on Processors in this DPA shall apply to Company regardless of whether Company acts as a Processor or Subprocessor.

## **3. Company's Compliance.**

**3.1.** Company warrants and undertakes to process Passage Personal Data only for the limited and specified purposes set out in the Agreement and/or as otherwise lawfully instructed by Passage in writing (email or otherwise), except where otherwise required by applicable law. Company will immediately inform Passage if, in its opinion, an instruction is in breach of Applicable Privacy Laws.

**3.2.** Subject to Section 5 of this DPA, where Company transfers Passage Personal Data originating from the European Union, the European Economic Area, and/or their member states, the United Kingdom and Switzerland, to a country that does not provide

an adequate level of data protection within the meaning of the applicable laws and regulations the foregoing named areas, Company warrants and agrees to: (i) comply with its obligations under Applicable Privacy Laws; and (ii) provide at least the same level of protection to Passage Personal Data as is required by the Privacy Shield Principles and/or as Passage may otherwise reasonably require, in accordance with Applicable Privacy Laws, to ensure an adequate level of protection for Passage Personal Data. Company agrees to notify Passage promptly in writing of its inability to meet its obligations under this Section 3.2 and to take all reasonable and appropriate measures to remedy any non-compliance and/or cease processing Passage Personal Data, as determined by Passage in its sole discretion. Where Company has not certified to the Privacy Shield Framework Principles, Company warrants and agrees to: (i) the SCCs, which are hereby incorporated into this DPA; and (ii) implement the technical and organizational security measures specified in Section 12 before processing the Passage Personal Data.

#### **4. Description of Processing.**

Personal Data will be processed strictly in accordance with the terms of this DPA for purposes of providing the Services and otherwise agreed to in the Agreement and any applicable writing signed by both Parties. Without limiting the generality of the foregoing, the subject matter, nature, and purpose of the processing under this DPA is the provision of the Services under the Agreement, and the categories of personal data and categories of data subjects are those necessary to provide the Services under the Agreement, as described more fully in the Agreement. The Parties acknowledge and agree that the description of processing as set out in this paragraph is accurate:

- 4.1. Subject matter of the processing. The processing of any Passage Personal Data by the Company in the provision of Services specified in the Agreement.
- 4.2. Duration of the processing. Company shall possess the relevant Passage Personal Data only for as long as necessary to carry out its obligations under any Applicable Privacy Laws, the terms of this DPA, and/or the Agreement.
- 4.3. Nature and purpose of the processing. Company will process Personal Data as necessary to provide the Services pursuant to the Agreement, and as further instructed by Passage.
- 4.4. Type of Personal Data being processed. The Personal Data of the customers, prospective customers, and end users of Passage's various service offerings may include, without limitation, name, company/organization name, issue affiliation data, Internet cookies, connection/relationship data, event and survey/petition registration/attendance/response data, email address, IP address, geolocation data, credit card and payment information, browser data, navigational data (including website usage information), Salesforce usage data, and data relating to the usage of Passage's various service offerings.
- 4.5. Categories of data subjects being processed. Passage may submit Personal Data to Company, to the extent which is determined and controlled solely in Passage's discretion, which may include, but is not limited to the following categories of data subjects: Passage's prospective customers, current customers, end users, and former customers.

#### **5. Instructions.**

Company may only act and process the Personal Data in accordance with the documented instruction from Passage (the “Instruction”). The Instruction at the time of entering into this DPA is that Company may only process the Personal Data with the purpose of delivering the Services as described herein and within the Agreement. Company shall give written notice without undue delay if Company considers, at the time, the Instruction to be in conflict with the Applicable Privacy Laws.

## **6. Confidentiality and Security.**

**6.1.** Company shall ensure that any person that it authorizes to process the Passage Data (including Company’s staff, agents and subcontractors) shall be subject to a duty of confidentiality.

**6.2.** Company shall ensure it implements and maintains throughout the term of the Agreement, or duration of its Services to Passage as a Processor or Subprocessor, appropriate technical and organizational measures to protect Passage Data, including protection against Data Breaches. Where Passage is Privacy Shield certified, such measures shall comply with the Privacy Shield Principles

## **7. Subprocessing.**

Company shall notify Passage of any Subprocessors it uses in respect of Passage Personal Data, and Company shall: (i) ensure that any Subprocessor is contractually bound in writing to provide at least the same level of protection as is required by this DPA and complies with Applicable Privacy Laws; (ii) be fully responsible for, and liable to Passage for acts and omissions of any Subprocessor as if they were Company’s own act or omission; and (ii) provide Passage with details of any Subprocessors appointed.

## **8. Cooperation with the Data Rights Subject.**

Company will provide all assistance reasonably required by Passage to enable Passage to: (i) respond to, comply with, or otherwise resolve any request, question or complaint received by Passage (or a Passage customer or prospective customer) from: (a) any living individual whose Personal Data is processed by Company on behalf of Passage; or (b) any applicable formally designated data protection authority; and (ii) comply with (and demonstrate compliance with) its obligations under Applicable Privacy Laws. In the event that any such request, question or complaint under this Section is made directly to Company, Company shall inform Passage providing full details of the same within 48 hours of receiving notice thereof.

## **9. Audit.**

On reasonable prior written notice, Company agrees to provide Passage (or its appointed auditors) with all information Passage deems reasonably necessary for Passage to audit Company’s compliance with the requirements of this DPA, including completion of audit questionnaires, provision of security policies and summaries of assessments of compliance with any industry standards (e.g., ISO 27001, SSAE 16 SOC II), penetration testing and vulnerability scans.

## **10. Data Breach.**

In the event of a Data Breach, Company will take, at a minimum, the following actions (unless authorized in writing by Passage):

- 10.1. Promptly notify Passage without undue delay (and at latest within 48 hours of becoming aware of the Data Breach) and provide Passage with a reasonably detailed description of the Data Breach, the type of data that was the subject of the Data Breach and the identity of each affected person as soon as such information can be collected or otherwise becomes available, as well as any other information that Passage may reasonably request relating to the Data Breach; and
- 10.2. Promptly (and latest beginning within 24 hours of becoming aware of the Data Breach) investigate the Data Breach, make reasonable efforts to mitigate the effects and harm of the Data Breach in accordance with its obligations under Section 3 above, and provide any other assistance that Passage may reasonably request relating to the Data Breach.

### **11. Deletion or Return of Passage Data.**

Upon termination or expiry of this DPA, Company shall (at Passage's election) destroy or return to Passage all Passage Data (including all copies of Passage Data) in its possession or control (including any Passage Data subcontracted to a third-party for processing), unless any applicable law requires Company to retain Passage Data.

### **12. Technical or Organizational Security Measures Requirement.**

#### **12.1. Policies for information security.**

Company agrees to implement a set of policies for information security that are defined, approved by management, published and communicated to employees and relevant external parties.

#### **12.2. Information security awareness, education and training.**

Company shall ensure all of its employees and, where relevant, contractors receive appropriate awareness, education, training, and regular updates in organizational policies and procedures, as relevant for their job function.

#### **12.3. Acceptable use of assets.**

Company will ensure rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.

#### **12.4. Classification of information.**

Company will ensure all information assets are classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

#### **12.5. Disposal of media.**

Company will ensure that, when no longer needed, all media is disposed of using formal procedures.

#### **12.6. Access control policy.**

Company will ensure an access control policy is established, documented, and reviewed based on business and information security requirements.

#### **12.7. Policy on the use of cryptographic controls.**

Company shall ensure a policy on the use of cryptographic controls for protection of information has been developed and implemented.

**12.8. Secure disposal or re-use of equipment.**

Company will ensure all items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

**12.9. Controls against malware.**

Company will implement detection, prevention and recovery controls to protect against malware, combined with appropriate user awareness.

**12.10. Information backup.**

Company will implement a backup policy to define the organization's requirements for backup of information, software, and systems.

**12.11. Network controls.**

Company will ensure networks are managed and controlled to protect information in systems and applications and ensure groups of information services, users and information systems are appropriately segregated.

**12.12. Electronic messaging.**

Company will ensure information involved in electronic messaging will be appropriately protected.

**12.13. Confidentiality or non-disclosure agreements.**

Company will ensure requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information are identified, regularly reviewed, and documented.

**12.14. Securing application services on public networks.**

Company will ensure information involved in application services passing over public networks is protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

**12.15. Reporting and responding to information security events.**

The data importer will ensure information security events are reported through appropriate management channels as quickly as possible and will ensure information security incidents are responded to in accordance with the documented procedures.

**12.16. Planning information security continuity.**

Company will determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

**13. Indemnification.**

Company shall indemnify, keep indemnified and hold harmless Passage, its members, managers, customers and clients, officers, directors, employees, contractors, agents, representatives and Affiliates (each an "Indemnified Party") from and against all third-party loss, harm, cost (including legal fees and reasonable expenses), expense and liability that an Indemnified Party may suffer or incur as a result of Company's non-compliance with the requirements of this DPA.

**14. Limitation of Liability.**

In no event shall the aggregate liability of Passage together with all of its Affiliates arising out of or related to this DPA or Agreement exceed the total amount paid by Passage to Company hereunder for the Services giving rise to the liability in the twelve (12) months preceding the

first incident out of which the liability arose. The foregoing limitation will apply whether an action is in contract or tort and regardless of the theory of liability. Company shall be liable for the acts and omissions of its Subprocessors to the same extent Company would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

**15. Miscellaneous.**

Except for the changes made by this DPA, the Agreement, and/or any other agreements related to the Services remain unchanged and in full force and effect. With respect to provisions regarding processing of Personal Data, in the event of a conflict between the Agreement and this DPA, the provisions of this DPA shall control. In the event of a conflict between this DPA and any other provision of the Agreement between the Parties, this DPA will control; except where the Parties have individually negotiated data processing terms that are different from this DPA and which meet the requirements of Applicable Privacy Laws in full, in which case those negotiated terms will control.

**16. Governing Law.**

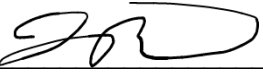
This DPA is governed by and construed under the laws of the State of Illinois, without reference to its conflict of laws provisions. Any dispute or claim arising out of or relating to the DPA or claim of breach hereof shall be brought exclusively in the federal court for the Northern District of Illinois or in the Circuit Court of Lake County, Illinois. By execution of the Agreement, the Parties hereby consent to the exclusive jurisdiction of such courts, and waive any right to challenge jurisdiction or venue in such courts with regard to any suit, action, or proceeding under or in connection with the DPA.

**17. Compliance with the Laws.**

The Parties agree to comply with their respective obligations under Privacy Laws. In particular, Company warrants and represents (on its behalf and on behalf of each of its affiliates where applicable) that it has obtained all necessary authorizations and consents required for compliance with Privacy Laws prior to disclosing, transferring, or otherwise making available any Personal Data to Company and that it has provided appropriate notifications to data subjects describing the purpose for which their personal data will be used pursuant to this DPA and MSA.

*[Signature page to follow]*

IN WITNESS WHEREOF, the Parties have executed this DPA as of the date first above written.

PASSAGE	COMPANY
<p><i>Brent Gossett</i></p> <hr/>	<hr/>
<p>Brent Gossett, on behalf of Passage Technology, LLC</p>	<p>Print Name: _____</p>
	<p>Signing on behalf of: _____</p>
<p>Jerry Reid, on behalf of Passage Technology, LLC</p>	<p><b>Email</b></p>
<p><b>Email</b> llc-members@passagetech.com</p>	<p><b>Mailing Address</b></p>
<p><b>Corporate Mailing Address</b> 100 S. Saunders Rd Suite 150 Lake Forest, IL 60045</p>	<p><b>Phone</b></p>
<p><b>Phone</b> 224-552-0083</p>	



## Schedule 1 – Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organization:

Passage Technology, LLC  
100 S. Saunders Rd., Suite 150 Lake Forest, IL 60045  
224-552-0077

(the “data exporter”)

And

Name of the data importing organization:

Company Name: \_\_\_\_\_  
Company Address: \_\_\_\_\_  
Company Phone: \_\_\_\_\_

(the “data importer”) each a ‘party’; together ‘the parties’, HAVE AGREED on the following Contractual Clauses (the “Clauses”) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in this Appendix 1.

### **Clause 1** **Definitions**

For the purposes of the Clauses:

- (a) “personal data”, “special categories of data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority” shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>1</sup>;
- (b) “the data exporter” means the controller who transfers the personal data;
- (c) “the data importer” means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

---

<sup>1</sup> Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

- (d) “the subprocessor” means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) “the applicable data protection law” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) “technical and organizational security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Clause 2**  
**Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

**Clause 3**  
**Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**Clause 4**  
**Obligations of the data exporter**

The data exporter agrees and warrants:

- (a) That the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) That it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) That the data importer will provide sufficient guarantees in respect of the technical and organizational security measures in place;
- (d) That after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) That it will ensure compliance with the security measures;
- (f) That, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) To forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) To make available to the data subjects upon request a copy of the Clauses and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) That, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) That it will ensure compliance with Clause 4(a) to (i).

**Clause 5**

## Obligations of the data importer<sup>2</sup>

The data importer agrees and warrants:

- (a) To process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) That it has implemented the technical and organizational security measures specified in the Data Processing Agreement before processing the personal data transferred;
- (d) That it will promptly notify the data exporter about:
  - i. Any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
  - ii. Any accidental or unauthorized access; and
  - iii. Any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
- (e) To deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) At the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) To make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information;
- (h) That, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

---

<sup>2</sup> ) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (i) That the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) To send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

**Clause 6**  
**Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

**Clause 7**  
**Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**Clause 8**  
**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2 within this clause. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

### **Clause 9** **Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

### **Clause 10** **Variation of the Contract**

The parties may not vary or modify the Clauses unless agreed to in writing and signed by the parties. This does not preclude the parties from adding clauses on business-related issues where required as long as they do not contradict or broaden data importer's obligations under the Clause.

### **Clause 11** **Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

### **Clause 12**

#### **Obligation After the Termination of Personal Data Processing Services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor agree that upon request of the data exporter and/or of the supervisory authority, each will submit its data processing facilities for an audit of the measures referred to in Clause 12 paragraph 1.

## Appendix 1 to the Standard Contractual Clauses

This Appendix 1 forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix 1.

### Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the authorized legal entity that has agreed to the Standard Contractual Clauses as a data exporter.

### Data importer

The data importer is (please specify briefly activities relevant to the transfer):

A provider of cloud software and data storage services, which processes personal data at the instruction of data exporter in accordance with the terms of the DPA.

### Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may transfer Personal Data to the Service at its sole discretion as controlled by data exporter, which may include data regarding the following categories: (1) customers, business partners, vendors, and prospects (who are natural persons); (2) data exporter's users, supporters, prospective users, and prospective supporters, authorized by data exporter to use the Services (who are natural persons); (3) data exporter's affiliates, advisors, agents, and freelancers.

### Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Service to the extent that, under data exporter's sole discretion and control, may include the following categories of Personal Data:

- First and Last Name
- Contact Information
- Professional life data
- Personal life data
- Connection/relationship data
- Locational data
- Event and survey/petition registration, attendance, and response data
- Issue affiliation data
- Internet cookies
- Usage information related to the Service



**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

Except where Union or Member State law provide that a data subject may not consent to any of the items in the following list, data exporter may submit special categories of data to the Service to the extent that, under data exporter's sole discretion and control, and which is, for the sake of clarity,

Personal Data with information revealing one or more of the following categories of Personal Data:

- Political party affiliation, participation, voting, contribution, and opinion data
- Religious belief and organization donation data
- Philosophical belief data
- Trade union membership data
- Ethnic data

The specified purposes for processing data in the special categories are: to provide the Service to Data Subject in accordance with the Agreement and for improving the Service for all users and customers.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The purpose of Processing the Personal Data is to provide the Service to Data Subject in accordance with the Agreement.