ALPHASENSE DATA PROCESSING ADDENDUM

This Data Processing Addendum, including the Standard Contractual Clauses referenced herein (“**DPA**”), amends and supplements any existing and currently valid agreements for services, orders, order forms, purchase orders, or other similar documents or agreements (the “**Service Agreement**”) either previously or concurrently made between **AlphaSense, Inc.**, with an address at 24 Union Square East, 6th Floor, New York, NY 10003 (“**AlphaSense**”), and the customer entity that is a counterparty to such Service Agreement (“**Customer**”). AlphaSense and Customer may individually be referred to as a “Party” and collectively as the “Parties”. For purposes of this DPA, “**Affiliate**” shall mean any entity directly or indirectly controlling, controlled by, or under common control with the applicable party. Defined terms used herein but not otherwise defined shall have the meanings set forth in the Service Agreement. This DPA is incorporated by reference into the Service Agreement, and the terms set out herein supersede any conflicting provisions of the AlphaSense Privacy Policy that may otherwise apply to the processing of Customer Personal Data (as defined below).

1. DEFINITIONS.

1.1. References to **Personal Data**, **Data Subject**, **Data Controller**, **Data Processor**, **Processing**, or **Personal Data Breach** shall be as defined in equivalent or substantially the same definitions under the Applicable Laws.

1.2. “**Applicable Laws**” means any applicable laws and regulation in any relevant jurisdiction relating to the data protection, data privacy, use or processing of any Personal Data under this DPA that apply to a Party, including where applicable: (i) EU Regulation 2016/679 ("**GDPR**"); (ii) any laws or regulations ratifying, implementing, adopting, supplementing or replacing such applicable laws and regulation, in each case, as updated, amended or replaced from time to time; (iii) the GDPR as incorporated into law in the United Kingdom pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Data Protection Act 2018 ("**DPA 2018**"), the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419), or any other statute or statutory provision which modifies, consolidates, re-enacts or supersedes the GDPR following the cessation of application of European Union law to the United Kingdom as a result of the withdrawal of the United Kingdom from the European Union; the Swiss Federal Act on Data Protection (“**FADP**”),and the “**California Data Protection Law**” means the California Consumer Privacy Act (“CCPA”) Cal. Civ. Code § 1798.100 et seq., and its implementing regulations as in effect until January 1, 2023; as of January 1, 2023, any reference to the CCPA shall be construed as a reference to the California Privacy Rights Act (“CPRA”) Cal. Civ. Code section 1798.100 et seq., and its implementing regulations, as in effect from January 1, 2023; and the Massachusetts Right of Privacy Act, and other applicable state data security laws, and any and all applicable laws relating to breach notification in connection with Personal Data.

1.3. “**Customer Personal Data**” shall mean the Personal Data that is provided or uploaded by the Customer, or which is otherwise Processed by AlphaSense as a Data Processor on behalf of Customer or one of its Affiliates as a Data Controller.

1.4. “**Standard Contractual Clauses**" or "**SCCs**” means the approved version of standard contractual clauses for transfers of personal data in countries not otherwise recognised as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time) which is set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 and at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj as may be updated from time to time by the European Commission or the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses.

1.5. “**Sub-processor**” means any third party engaged by AlphaSense (including any AlphaSense Affiliate) to process Customer Personal Data on behalf of Customer.

2. EU, EEA, UK DATA PROTECTION LAWS.

Both Parties will comply with their respective obligations under the Applicable Laws as relevant to this DPA (and where an Affiliate of a Party is the Data Controller or Data Processor, such Party shall ensure that its Affiliate complies with the Applicable Laws). This DPA is in addition to, and does not relieve, remove or replace, a Party's obligations under the Applicable Laws. In the event of any conflict between the terms of this DPA or the Applicable

Laws, the Applicable Laws will govern.

2.1. **Processing of Personal Data and Description of Transfer.** The Parties acknowledge that for the purposes of the Applicable Laws, the Customer is the Data Controller and AlphaSense is the Data Processor in respect of the Customer Personal Data. Customer shall not require AlphaSense to undertake or engage in any processing activity that would require AlphaSense to act as a Data Controller or would result in a determination that AlphaSense has acted in the capacity of a Data Controller with respect to any Customer Personal Data. The following sets forth the description of transfer and details of the Customer Personal Data and Processing to be undertaken by AlphaSense on behalf of Customer:

Scope and frequency of the transfer	Processing of the Customer Personal Data pursuant to the Service Agreement for provision of the products, services and support services on a continuous basis
Nature of Processing	Transfer, storage, hosting and such other processing activities that are required to provide and support the products, and as otherwise set out in this DPA or specified by the Customer.
Purpose of Processing	The provision of products, services and support services to the Customer.
Duration of the Processing	The duration of the Term (as defined below), or as required to make relevant Customer Personal Data available to Customer, or such other period as required by Applicable Laws, whichever is longer.
Retention Period	As necessary for performance of obligations under the Services Agreement or as required by Applicable Laws, whichever is longer.
Types of Personal Data	The Customer Personal Data (as defined above) which may include but not be limited to name, email address, IP address, phone number and job title.
Categories of Data Subject	The Customer’s personnel, contractors, suppliers and related third parties.

2.2. Without prejudice to the generality of Section 2.1, the Customer will ensure that it (or its Affiliate) has a legal basis for Processing, including all necessary and appropriate consents and notices, to enable the lawful transfer of the Personal Data to AlphaSense for the duration and purposes of this DPA.

2.3. AlphaSense shall process the Customer Personal Data in accordance with the written instructions of the Customer (as detailed in Section 2.1 above and this DPA) unless AlphaSense is otherwise required by Applicable Laws, in which case such Processing shall be carried out in accordance with such laws (and AlphaSense will provide notice of such Processing to Customer to the extent permitted by Applicable Laws. Confirming acceptance to these terms shall constitute the Customer’s written instructions for AlphaSense to undertake the Processing detailed in this DPA and Section 2.1. AlphaSense shall not publish, disclose, retain, sell, or divulge any Customer Personal Data to any third party for any purposes (save for Sub-processors appointed pursuant to section 2.11 herein) without the Customer’s prior written consent (such approval not to be unreasonably withheld or delayed), unless communication or disclosure is required by Applicable Laws or by any court or other authority of competent jurisdiction, provided that, to the extent lawfully permitted, AlphaSense first provides notice to the Customer and such communication does not refer to the Customer (unless legally required).

2.4. AlphaSense shall ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful Processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, appropriate and proportionate to the harm that might result from the same, having regard to the state of technological development and the cost of implementing any measures which shall include the measures set out in the Appendix of this DPA.

2.5. AlphaSense shall, in relation to any Customer Personal Data Processed in connection with the performance by AlphaSense of its obligations under this DPA and to the extent required by Applicable Laws:

2.5.1. ensure that all personnel who have access to and/or process Personal Data are required to keep the

Personal Data confidential or are under an appropriate statutory obligation of confidentiality with obligations substantially similar as those contained in this DPA; and

2.5.2. taking into account the nature of the Processing and the information available to AlphaSense, assist the Customer, at the Customer's cost, in responding to any request from a Data Subject under Applicable Laws and in ensuring compliance with its obligations under the Applicable Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators, as applicable;

2.5.3. notify the Customer without undue delay on becoming aware of a Personal Data Breach;

2.5.4. on expiry of the Retention Period, delete or return Customer Personal Data and copies thereof to the Customer unless required by Applicable Laws to continue to store the Customer Personal Data (in which case AlphaSense shall retain the same as required by the applicable law and its confidentiality obligation under this DPA); and

2.5.5. make available to the Customer (on reasonable request) all information necessary to demonstrate AlphaSense's compliance with its obligations under this Section 2.5 and subject to AlphaSense's reasonable security procedures, business and operational requirements and AlphaSense's confidentiality obligations, allow for audits, including inspections, conducted by the Customer, its supervisory authority or regulator, at the Customer's own cost and expense, upon the Customer giving AlphaSense prior written notice of no less than thirty (30) days of its intent to conduct such an audit or inspection. For the avoidance of doubt, such audit and inspection shall only be for the purposes of determining AlphaSense's compliance with its obligations under this DPA and shall not be conducted more than once every twelve (12) months.

2.6. **Cross-border transfers of personal data** AlphaSense (and any Sub-processor) must not transfer or otherwise process the Personal Data outside the EEA without obtaining the Customer's prior written consent. Where such consent is granted, AlphaSense may only process, or permit the processing, of the Personal Data outside the EEA under the following conditions:

2.6.1.AlphaSense is processing the Personal Data in a territory which is subject to adequacy regulations under the Applicable Laws and the territory provides adequate protection for the privacy rights of individuals; or

2.6.2.AlphaSense participates in a valid cross-border transfer mechanism under the Applicable Laws, so that AlphaSense (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR and EU GDPR; or

2.6.3.the transfer otherwise complies with the Applicable Laws for the reasons set out in this DPA.

2.7. **Transfers of EU Personal Data**. The Parties acknowledge and agree that Processing of the Personal Data will occur in the United States and possibly other jurisdictions outside the residence of the Data Subjects, and AlphaSense shall comply with all notice and consent requirements for such transfer and Processing to the extent required by Applicable Laws. Where there is a transfer of Personal Data by a data exporter from within the EEA to a data importer outside the EEA, and such transfer is not governed by an "adequacy decision", and is not otherwise "subject to appropriate safeguards" and no "derogation for specific situations" applies, each within the meanings given to them in Articles 45, 46 and 49 of the GDPR respectively (an "**ex-EEA Transfer**"), the ex-EEA Transfer shall be governed by the SCCs. The terms of the SCCs, together with Annex I and II set out in **Exhibit A,** and Annex III set out in **Exhibit B** to this DPA, are incorporated in this DPA by this reference solely as required by Applicable Laws with respect to EU Personal Data transferred out of the EU in connection with AlphaSense's performance of the Services, and executed by the parties with AlphaSense as the 'Data Importer' and the Customer as the 'Data Exporter' with effect from the commencement of the relevant transfer. By signing the Services Agreement, AlphaSense and Customer shall be deemed to have signed and accepted the EU Controller to Processor SCCs and:

2.7.1.Module 2 of the SCCs applies to transfers of Personal Data from Customer (as a controller) to

AlphaSense (as a processor).

2.7.2. Clause 7 – Docking clause of the EU Controller to Processor SCCs shall not apply;

2.7.3. Clause 9 – "Option 2" shall apply and the “time period” shall be 30 days;

2.7.4. Clause 11(a) – Redress of the EU Controller to Processor SCCs, the optional language shall not apply;

2.7.5. Clause 13(a) – Supervision of EU Controller to Processor SCCs, the following shall be inserted: Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

2.7.6. Clause 17 – Governing law of the EU Controller to Processor SCCs. These Clauses shall be governed by the law of Ireland.

2.7.7. Clause 18 – Choice of forum and jurisdiction of the EU Controller to Processor SCCs shall be Ireland.

2.7.8. Annex I of the EU Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of clause 2.1 of this DPA and the processing operations are deemed to be those described in the Services Agreement;

2.7.9. Annex II of the EU Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of Exhibit A to this DPA.

2.7.10. Annex III of the EU Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of Exhibit B to this DPA.

2.8. **Transfers of UK Personal Data**. Where there is a transfer of Personal Data by a data exporter from within the UK to a data importer outside the UK and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the DPA 2018 (an "**ex-UK Transfer**"), then, subject to the remaining provisions of this section 2.8, the SCCs shall apply to such ex-UK Transfer in the same way as set out in section 2.7 for ex-EEA Transfers, save that the following amendments to the application of the SCCs for these purposes shall apply (with references in this section 2.8 to Clauses being to Clauses of the SCCs):

2.8.1. the SCCs shall be read and interpreted in the light of the provisions of the UK GDPR and the DPA 2018, and so that they fulfil the intention for them to provide appropriate safeguards as required by Article 46 of UK GDPR;

2.8.2. the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the UK GDPR and the DPA 2018;

2.8.3. the SCCs are deemed to be amended to the extent necessary so they operate:
2.8.3.1. for ex-UK Transfers made, to the extent that the UK GDPR and the DPA 2018
2.8.3.2. apply to AlphaSense's processing when making that ex-UK Transfer; and
2.8.3.3. to provide appropriate safeguards for the ex-UK Transfer in accordance with Articles 46 of the UK GDPR Laws; and

2.8.4. without prejudice to the generality of sections 2.8.1, 2.8.2 and 2.8.3 SCCs are amended as follows:
2.8.4.1. Clause 6 Description of the transfer(s) is replaced with:
“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where the

Applicable Laws in the UK apply to the data exporter's processing when making that transfer.";

2.8.5. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK GDPR and DPA 2018" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR and DPA 2018;

2.8.6. References to Regulation (EU) 2018/1725 are removed;

2.8.7. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

2.8.8. Clause 13(a) and Annex I.C are not used; the "competent supervisory authority" is the ICO;

2.8.9. Clause 17 is replaced to state "*These Clauses are governed by the laws of England and Wales*";

2.8.10. Clause 18 is replaced to state:
"*Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts*".

2.9. AlphaSense's liability under the SCCs shall form part of AlphaSense's liability under the Service Agreement, and shall be subject to any exclusions and limitations on AlphaSense's liability set out in the Service Agreement.

3. **Conflicts**. If there is any conflict or ambiguity between the terms of this DPA and the SCCs, the term contained in the SCCs shall have priority (but only to the extent and in respect of the transfer, and not in respect of any other processing activity). In the event of any conflict or inconsistency between this DPA and Applicable Laws, Applicable Laws shall prevail. In the event of any conflict or inconsistency between the terms of this DPA and the terms of the Services Agreement, the terms of this DPA shall prevail solely to the extent that the subject matter concerns Personal Data, data protection, data privacy and data security.

4. **Sub-processors**. The Customer hereby consents to AlphaSense appointing third-party sub-processors of Customer Personal Data under this DPA, provided that:

4.1. The Customer has provided its prior written consent for appointment of such Sub-processor or Sub-processor is an Affiliate of AlphaSense or identified in AlphaSense's list of Sub-processors as specified at https://trust.alpha-sense.com/ **Exhibit B**, as updated by AlphaSense from time to time and notified to the Customer;

4.2. Within 10 working days of AlphaSense notifying the Customer of any additions to the Sub-processors list in writing, the Customer may object in writing to use of a Sub-processor, and shall describe its reasons for the objection, and may request corrective steps to be taken. If the Customer objects to the use of a Sub-processor then the Customer will have the option to utilise the Services without the portion of Services provided by that Sub-processor or, to the extent the foregoing is not reasonably practical or possible, terminate the portion of the Services that utilizes the Sub-processor; and

4.3. AlphaSense has entered into, or (as the case may be) will enter into with the third-party sub-processor a written agreement incorporating terms which are substantially similar to those set out in this DPA. AlphaSense acknowledges and agrees that it remains responsible to the Customer for any breach of the terms of this DPA by any Sub-processor.

5. **California Privacy Rights**. For purposes of California Data Protection Law, Customer shall be considered the Business and AlphaSense shall be considered the Service Provider.

5.1. Customer discloses Personal Information to AlphaSense solely for the purpose of AlphaSense's provision of the Services contemplated under the Services Agreement, exclusively for Customer's business purposes specified therein.

5.2. AlphaSense will reasonably cooperate and assist Customer with meeting the Customer's CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of AlphaSense 's processing and the information available to AlphaSense.

5.3. AlphaSense must notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA. Specifically, AlphaSense must notify the Customer within 5 working days if it receives a verifiable consumer request under the CCPA.

5.4. AlphaSense shall: (i) not sell or share Personal Information; (ii) not retain, use, or disclose the Personal Information: (A) outside the direct business relationship between AlphaSense and Customer; or (B) for any purpose other than for the business purposes specified in the Services Agreement, unless otherwise permitted by the California Data Protection Law; (iii) upon instruction by Customer, stop using Sensitive Personal Information for any purpose other than providing the Services to the extent AlphaSense has actual knowledge that the Personal Information is Sensitive Personal Information; (iv) not combine Customer Personal Information with other Personal Information that AlphaSense receives from, or on behalf of, another person or collects from its own interaction with consumers, unless permitted by California Data Protection Law; (v) refrain from attempting to re-identify any de-identified information disclosed by Customer to AlphaSense under the Services Agreement; (vi) only subcontract any Processing of Personal Information pursuant to Section 4 of this DPA (“Sub-Processors”), and, to the extent commercially feasible, enable Customer to be promptly notified if AlphaSense’s Sub-Processor further subcontracts any Processing of Personal Information; (viii) assist Customer in responding to verifiable consumer requests pursuant to Section 2.5.2 of this DPA; (ix) refrain from complying with consumer deletion request submitted directly to AlphaSense to the extent that AlphaSense has collected, used, processed, or retained the Personal Information in its role as Service Provider to Customer; (x) promptly notify Customer if AlphaSense determines that it can no longer meet its obligations under California Data Protection Law or under this Section; and (xi) remain liable for AlphaSense’s own violations of California Data Protection Law. “Business,” “Personal Information,” “Selling,” “Sensitive Personal Information,” “Services” and “Service Provider” as used in this Section shall have the meaning set forth in California Data Protection Law.

6. **Switzerland.** For transfers of Personal Data that are subject to the FADP, the SCCs form part of this DPA as set forth in Section 2.7 of this DPA, but with the following differences to the extent required by the FADP:

6.1. References to the GDPR in the SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

6.2. The term “member state” in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs.

6.3. References to personal data in the SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

6.4. Under Annex I(C) of the SCCs (Competent supervisory authority):

6.5. Where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

6.6. Where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in Section 7(b)(viii) of this DPA insofar as the transfer is governed by the GDPR.

6.7. To the extent the SCCs apply, nothing in this DPA or the Agreement shall be construed to prevail over any conflicting clause of the SCCs. Each party acknowledges that it has had the opportunity to review the SCCs.

7. **General.** This DPA is without prejudice to the rights and obligations of the Parties under the Services Agreement which shall continue to have full force and effect.

7.1. This DPA together with the Services Agreement is the final, complete and exclusive agreement of the Parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the Parties with respect to such subject matter.

7.2. To the extent that it is determined by any data protection authority that the Services Agreement or this DPA is insufficient to comply with Applicable Laws or changes to Applicable Laws, AlphaSense and Customer agree to cooperate in good faith to amend the Services Agreement or this DPA or enter into further mutually agreeable data processing agreements in an effort to comply with all Applicable Laws.

8. **Term.** This Agreement will remain in full force and effect so long as the Services Agreement remains in effect (“Term”).

Exhibit A: ANNEX I and ANNEX II to the Standard Contractual Clauses

(These Annexes form part of the Standard Contractual Clauses)

ANNEX I

A. Data exporter and Data importer

The data exporter is Customer, a customer of Services provided by AlphaSense. The data importer is AlphaSense, a provider of software services. AlphaSense processes Personal Data upon the instructions of the data exporter in accordance with the terms of the Services Agreement and the DPA.

B. Description of Transfer

As set out in the table at clause 2.1 of this Data Processing Addendum.

C. Competent Supervisory Authority

The Data Protection Commissioner of the Republic of Ireland.

ANNEX II

AlphaSense will maintain reasonable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data transferred to Processor as described in the Services Agreement to ensure a level of security appropriate to the risk.

AlphaSense shall exercise reasonable efforts to implement the following measures in connection with information security of Customer Personal Data:

a) backing-up the Customer Personal Data at regular intervals;

b) ensuring that AlphaSense is able to restore lost or damaged Customer Personal Data from the latest back-up;

c) not using the Customer Personal Data except as required for the performance of its obligations under the Services Agreement;

d) upon Customer’s written request, granting Customer access to SAE18 SOC 2/ISAE3402 SOC (Type II) or similar reports in respect of specific software supplied under the Services Agreement, and addressing data security requirements stated in this DPA;

e) complying with information management procedures and safeguards based on Good Industry Practice, including those concerning the security of the Customer Personal Data. For the purpose of this DPA, “Good Industry Practice” means that degree of skill, care and prudence which would ordinarily be expected of a skilled and experienced supplier of software products and services of the same or a similar nature to the Services and support services;

f) maintaining and enforcing safeguards against the destruction, loss, or alteration of Customer Personal Data that are no less rigorous than those maintained by AlphaSense for its own information of a similar nature or that otherwise comply with Good Industry Practice;

g) in the event of any destruction, loss, or reduction in the accessibility or usability of Customer Personal Data which is caused by AlphaSense, restoring such data using Good Industry Practice data restoration techniques;

h) taking all necessary precautions, in accordance with Good Industry Practice, to prevent any malicious code affecting the Services and the Customer Personal Data, including but not limited to using the latest versions of anti-malware software (including latest definitions and updates) available from an industry accepted anti-malware software vendor to check for and delete malicious code;

i) notifying the Customer as soon as practicable upon becoming aware of any Security Incident and providing the Customer with a detailed description of the Security Incident, the type of Customer Personal Data that is the subject of the Security Incident, the identity of any affected individuals and all other information and cooperation which the Customer may reasonably request. For the purpose of this DPA, "Security Incident" shall mean any incident resulting in loss, destruction or material alteration of Customer Personal Data, or unauthorized third-party access to Customer Personal Data;

j) taking immediate action, at AlphaSense's own cost, to investigate, identify, prevent and mitigate the effects of any Security Incident and, with the Customer's prior agreement, to carry out any recovery or other action necessary to remedy the Security Incident. AlphaSense must ensure that any such recovery or other action does not compromise any technical information or artefacts (including, for example, logs) which would reasonably be required by the Customer to understand the Security Incident, mitigate its effects and/or prevent its recurrence;

k) not issuing, publishing or otherwise making available to any third party any press release or other communication concerning a Security Incident without the Customer's prior approval (such approval not to be unreasonably withheld or delayed), unless communication is required by Applicable Laws or by any court or other authority of competent jurisdiction provided that before making such communication AlphaSense to the extent lawful provides notice to the Customer that it will be making such communication and such communication must not reference the Customer (unless legally required to do so);

l) using data centers where Customer Personal Data is stored, accessed or otherwise processed in accordance with Good Industry Practice;

m) keeping any Customer Personal Data in electronic form logically separated from other third parties;

n) ensuring that access to Customer Personal Data by AlphaSense's personnel is restricted on a strictly need to know basis and that all AlphaSense's personnel who are granted such access have completed appropriate security training;

o) performing continuous service improvement and continuous monitoring of the Services and promptly rectifying any security vulnerabilities identified by such testing;

p) implementing other measures or modifying any of the above to the extent reasonably necessary in AlphaSense's discretion.

Exhibit B: Annex III to the Standard Contractual Clauses

(This Annex forms part of the Standard Contractual Clauses)

ANNEX III

The Data exporter has authorized AlphaSense's use of the sub-processors, a list of which can be found at https://trust.alpha-sense.com/.