INSIGHTSOFTWARE
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA"), forms part of, and is subject to, the Master Terms or other written or electronic terms of service or subscription agreement (“Agreement”) between insightsoftware (as defined below) and Customer that references this DPA, and is effective as of the same date of the Agreement.

This DPA applies where, and to the extent that, insightsoftware processes Personal Data on behalf of Customer when providing Services under the Agreement. The parties agree that this DPA shall replace any existing DPA, or other data protection provisions the parties may have previously entered into in connection with the Services (as defined in the Agreement). Any capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

1.1 "**Affiliate**" means an entity that directly or indirectly controls, is controlled by or is under common Control with an entity. For purposes of this definition, "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question.

1.2 “**California Personal Information**” means Personal Data that is subject to the protection of the CCPA and any later amendments thereto, including by not limited to the California Privacy Rights Act of 2020.

1.3 "**CCPA**" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018) and any later amendments thereto, including by not limited to the California Privacy Rights Act of 2020.

1.4 "**Customer Data**" means any Personal Data that is uploaded for storage or hosting that insightsoftware processes on behalf of Customer in the course of providing the Services.

1.5 "**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

1.6 "**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

1.7 "**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

1.8 "**EEA**" means the European Economic Area.

1.9 "**EU Data Protection Law**" means all current data protection and privacy laws applicable to the processing of Personal Data under the Agreement including but not limited to (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**"); (ii) 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) ("**GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the Swiss Federal Data Protection Act; and (v) any national data protection laws made under or pursuant to (i) and (ii).

1.10 **“insightsoftware”** means insightsoftware, LLC or its affiliate that is a party to the Agreement.

1.11 **"Model Clauses"** means, as applicable,:

(a) in the respect of data relating to Data Subjects based in the European Union, the European Commission’s Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries as set out in the Annex to Commission Implementing Decision 2021/91, a completed copy of which comprises Attachment A; or

(b) in respect of the data relating to Data Subjects based in the United Kingdom, the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU as adapted for the UK, a completed copy of which comprises **Error! Bookmark not defined.**Attachment B or such alternative clauses as may be approved by UK law from time to time.

1.12 "**Personal Data**" means any information relating to an identified or identifiable natural person.

1.13 "**Processing**" has the meaning given to it in the GDPR and also includes 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. The terms "Process", "Processes" and "Processed" will be construed accordingly.

1.14 "**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

1.15 "**Sell**" or "**Sale**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means, Customer Data to a third party for monetary or valuable consideration.

1.16 "**Services**" has the meaning set forth in the Agreement.

1.17 "**Subprocessor**" means any Data Processor engaged by insightsoftware or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Subprocessors may include third parties or Affiliates of insightsoftware.

1.18 "**UK Data Protection Laws**" means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR, the UK Data Protection Act 2018 and regulations made thereunder.

1.19 "**UK GDPR**" has the meaning given to it in section 310 (as supplemented by section 205(4) of the UK Data Protection Act 2018.

2. Roles and Scope of Processing

2.1 Role of the Parties. As between insightsoftware and Customer, Customer is the Data Controller of Customer Data and insightsoftware will process Customer Data only as a Data Processor acting on behalf of Customer.

2.2 Customer Processing of Customer Data. Customer agrees that (i) it will comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to insightsoftware; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary for insightsoftware to process Customer Data pursuant to the Agreement and this DPA.

2.3 insightsoftware Processing of Customer Data. insightsoftware will process Customer Data only (i) for the purpose of providing the Services and in accordance with Customer's documented lawful instructions as set forth in the Agreement and this DPA; (ii) as part of the direct business relationship between Customer and insightsoftware; (iii) on behalf of Customer and insightsoftware's other customers, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity; or (iv) as required by law, provided insightsoftware will inform Customer of such legal requirement prior to commencing such processing unless prohibited by law. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in this DPA and the Agreement, which can be amended from time to time, either by an addendum to this DPA or the Agreement or by a commercial document signed between the parties.

3. Subprocessing

3.1 Authorized Subprocessors. Customer approves the grant of third party access for all current insightsoftware Subprocessors as of the last date of execution of this DPA. insightsoftware may in respect of Personal Data that is provided under this Agreement only authorize a new Subprocessor to process such Personal Data if the Customer is provided with the opportunity to object to the appointment of each Subprocessor to process such Personal Data within 7 working days after insightsoftware supplies the Customer with full details in writing regarding such Subprocessor.

3.2 Subprocessor Obligations. Where insightsoftware authorizes any Subprocessor:

(a) insightsoftware will restrict the Subprocessor's access to Customer Data solely to what is necessary to assist insightsoftware in providing or maintaining the Services, and will prohibit the Subprocessor from accessing Customer Data for any other purpose;

(b) insightsoftware will enter or has already entered into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Customer Data to the standard required by applicable Data Protection Laws and;

(c) insightsoftware will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause insightsoftware to breach any of its obligations under this DPA.

4. Security Measures and Security Incident Response

4.1 Security Measures. insightsoftware has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of Customer Data ("**Security Measures**"), as updated or replaced from time to time.

4.2 Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that insightsoftware may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

4.3 Personnel. insightsoftware restricts its personnel from processing Customer Data without authorization by insightsoftware as set forth in the Security Measures and shall ensure that any individual who is authorized by insightsoftware to process Customer Data is bound under appropriate obligations of confidentiality and non-use.

4.4 Customer Responsibilities. Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services. Customer may elect to implement technical or organizational measures in relation to Customer Data, which may include (i) protecting account authentication credentials; (ii) protecting the security of Customer Data when in transit to and from the Services; (iii) implementing measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and (iv) taking any appropriate steps to securely encrypt or pseudonymise any Customer Data uploaded to the Services.

4.5 Security Incident Response. Upon becoming aware of a Security Incident, insightsoftware will notify Customer without undue delay and will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. insightsoftware will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident.

5. Customer Audits

5.1 Reports. Upon request, insightsoftware will supply a summary copy of security audit report(s) ("**Report**") to Customer in accordance with the technical and organizational measures set forth in Attachment C, which reports shall be subject to the confidentiality provisions of the Agreement. insightsoftware will also respond to any reasonable written audit questions submitted to it by Customer to review insightsoftware's compliance with Data Protection Laws provided that Customer shall not exercise this right more than once per year.

5.2 Customer Audits. insightsoftware will permit the Customer and its third-party representatives to audit the insightsoftware's compliance with its Agreement obligations, on at least 60 days' notice, during the term of the Agreement. insightsoftware will give the Customer and its third-party representatives all necessary assistance to conduct such audits. Such audits shall be limited to once per year.

6. International Transfers

6.1 Data Center Locations. insightsoftware may transfer and process Customer Data anywhere in the world where insightsoftware, its Affiliates or its Subprocessors maintain data processing operations. insightsoftware will at all times provide an appropriate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

6.2 Transfers outside the EEA and/or UK. insightsoftware may only process, or permit the processing, of Personal Data outside the EEA and/or United Kingdom under the following conditions:

(a) insightsoftware is processing Personal Data, or permitting the processing of Personal Data in a territory which is subject to adequacy regulations under the EU Data Protection Laws and/or UK Data Protection Laws (as applicable) that the territory provides adequate protection for the privacy rights of individuals; or

(b) insightsoftware, its Affiliates and/or its Subprocessors (as applicable) enter into applicable Model Clauses so 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.

If any Personal Data transfer between the Customer and insightsoftware requires execution of Model Clauses in order to comply with the EU Data Protection Laws and/or UK Data Protection Laws (where the Customer is the entity exporting Personal Data relating to EU and/or UK based individuals to insightsoftware outside the EEA and/or UK), the Model Clauses attached at Attachment A and Attachment B are incorporated by reference and form part of this DPA. To the extent there is any ambiguity between this DPA and the Model Clauses, the Model Clauses shall prevail unless this DPA offers a Data Subject a greater level of protection in which case and only in respect of the greater protection that is offered this DPA shall prevail.

6.3 Alternative Data Export Solutions. Notwithstanding the foregoing, the parties agree that in the event insightsoftware adopts another alternative data export solution (as recognized under EU Data Protection Laws and/or UK Data Protection Laws (as applicable)), then the alternative data export solution shall apply instead of the Model Clauses. In the event that the alternative data export solution is later determined to not constitute an adequate level of data protection under EU Data Protection Laws, the Model Clauses shall apply as the data export solution; similarly, should such alternative data export solution later be determined not to constitute an adequate level of data protection under UK Data Protection Laws, the Model Clauses (or any equivalent recognized by Data Protection Laws) shall apply.

7. Return or Deletion of Data

7.1 General. Upon termination or expiration of the Agreement, insightsoftware will (at Customer's election) delete or return to Customer all Customer Data in its possession or control in accordance with the terms of the Agreement.

7.2 Exception. This requirement will not apply to the extent insightsoftware is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data insightsoftware will securely isolate and protect from any further processing, except to the extent required by law.

8. Cooperation

8.1 Access to Customer Data. To the extent that Customer is unable to independently access the relevant Customer Data within the Services and provided that Customer has configured the Services in accordance with insightsoftware's recommendations, insightsoftware will (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement when Customer is required to respond to such requests under applicable Data Protection Laws. In the event that any such request is made directly to insightsoftware, insightsoftware will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If insightsoftware is required to respond to such a request, insightsoftware will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 Law Enforcement Request. If a law enforcement agency sends insightsoftware a demand for Customer Data (for example, through a subpoena or court order), insightsoftware will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, insightsoftware may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then insightsoftware will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless insightsoftware is legally prohibited from doing so.

8.3 Legal Compliance. To the extent insightsoftware is required under Data Protection Law, insightsoftware will (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

9. Additional Provisions for California Personal Information

9.1 Roles of the Parties. When processing California Personal Information in accordance with Customer's Instructions, the parties acknowledge and agree that Customer is a "Business" and insightsoftware is a "Service Provider" for the purposes of, and as those terms are defined in, the CCPA.

9.2 Responsibilities. The parties agree that insightsoftware will Process California Personal Information as a "Service Provider" (as defined in the CCPA) strictly for the purpose of performing the Services under the Agreement or as otherwise permitted by the CCPA. insightsoftware shall provide commercially reasonable assistance to cooperate with the Customer's efforts to comply with applicable consumers' rights. insightsoftware shall, in accordance with the Agreement, not sell personal information and not retain, use, or disclose personal information for any purpose other than those specified in this Agreement. insightsoftware certifies that it understands the restrictions of this section 9.2 and will comply with these restrictions.

10. General

10.1 Limitation of Liability. For the avoidance of doubt, any claim or remedies the Customer may have against insightsoftware, any of its Affiliates and their respective employees, agents and subprocessors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iii) under EU Data Protection Law and/or UK Data Protection Law, including any claims relating to damages paid to a data subject, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Customer further agrees that any regulatory penalties incurred by insightsoftware in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce insightsoftware's liability under the Agreement as if it were liability to the Customer under the Agreement. Notwithstanding the foregoing, in no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10.2 Responsible Entity. Any claims against insightsoftware or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

10.3 Compliance. To the extent reasonably necessary to comply with changes to applicable Data Protection Laws or in response to guidance or mandates issued by any court, regulatory body, or supervisory authority with jurisdiction over insightsoftware, insightsoftware may modify, amend, or supplement the terms of this DPA. insightsoftware will endeavor to provide prior written notice of any such changes to Customer by posting a notice on insightsoftware's website.

10.4 Governing Law. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

10.5 Permitted Disclosure. Customer acknowledges that insightsoftware may disclose the privacy provisions in this DPA to the U.S. Department of Commerce, the Federal Trade Commission, a European Union supervisory authority, or any other U.S. or EEA (including UK) judicial or regulatory body upon their lawful request.

10.6 Precedence. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict. If there is any conflict between this DPA and the Model Clauses, then to the extent this DPA affords a data subject greater rights and protections than afforded under the Model Clauses, this DPA shall prevail; in all other situations (i.e. where the data subject is afforded equal or lesser rights and protections under this DPA) the Model Clauses shall prevail.

10.7 Severability. The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

insightsoftware

DocuSigned by:

By: David Woodworth

DFF00F65033B4B9...

Name: David Woodworth

Title: CFO

Date: 2/17/2022

Customer: ______________________________

By: ____

Name: _____________________________________

Title: ______________________________________

Date: ______________________________________

Attachment A - Model Clauses

EU STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) The Customer, as defined in the Agreement (the "data exporter"), and

(ii) insightsoftware, as defined in the DPA (the "data importer")

each a 'party'; together 'the parties', have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter**.**

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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 behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX of the EU STANDARD CONTRACTUAL CLAUSES in Attachment A

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I of the EU STANDARD CONTRACTUAL CLAUSES in Attachment A

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: The data exporter is the legal entity specified as "Customer" in the DPA.

Address: As indicated in the Agreement.

Contact person’s name, position and contact details: Contact details for the data exporter are specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The data exporter is a customer of the data importer. The data exporter provides personal data to the data importer in connection with the data importer’s provision of goods, products or services (as applicable) to the data exporter, which are provided in accordance with the Agreement.

Signature and date appear on the last page of these Sample Contractual Clauses

Role (controller/processor): Controller

Data importer(s):

1. Name: insightsoftware as defined in the DPA

2. Address: 8529 Six Forks Road, Suite 400, Raleigh, NC 27615, United States of America
Contact person’s name, position and contact details:

Legal Department, Attn: DPO

8529 Six Forks Road, Suite 400, Raleigh, NC 27615, United States of America
privacy@insightsoftware.com

Activities relevant to the data transferred under these Clauses: Performance of the Agreement pursuant to the instructions of the data exporter

Signature and date appear on the last page of these Sample Contractual Clauses

Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Data subjects may include:

- Users of the insightsoftware Software, Support Services, and/or Cloud Services (as defined in the Agreement);
- Employees, contractors and other agents of insightsoftware's customers;
- Suppliers; and
- With respect to Certent Equity Management software applications and services: Shareholders, former employees, and other equity participants accessing the insightsoftware's Software or Services under Customer's Subscription to Software, Support Services, or Cloud Services.

Categories of personal data transferred

The personal data transferred may include:

Data derived from use of the insightsoftware Software, Services, or Cloud Services including:

- Customer user details, which may include:
  - Name and surname;
  - Title and position;
  - Business email address; and
  - Business phone number.
- IT management and security details, which may include:
  - Connection data;
  - Log-in credentials: user name and passwords; and
  - IP address.
- Financial and transactional details, which may include:
  - Income;
  - Benefits;
  - Brokerage information;
  - Assets and investments; and
  - Bank account number.
- Human resources and employment details, which may include:
  - Social security number;
  - TaxID;
  - Trust information;
  - Home physical address;
  - Personal email address; and
  - Personal phone number.

- Other, which may include miscellaneous data uploaded to the Software, Services, or Cloud Services by Customer's users.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

In the normal, intended use case of the insightsoftware Software, Services, and Cloud Services, special categories of data should not be provided.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction of data, pursuant to the instructions of the Data Controller

Purpose(s) of the data transfer and further processing

Provision of insightsoftware Software, Services, and Cloud Services for the performance of the Agreement pursuant to the instructions of the data exporter

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration is specified in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The same as above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Dutch Data Protection Authority (Autoriteit Persoonsgegevens), the Netherlands

DATA EXPORTER	DATA IMPORTER
Name:..	Name:.. David Woodworth
Authorised signature:..........................	Authorised signature:.......................... DocuSigned by: David Woodworth DFF00F65033B4B9...

ANNEX II of the EU STANDARD CONTRACTUAL CLAUSES in Attachment A

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Please see Attachment C for the insightsoftware Security Provisions

Attachment B

UK Standard Contractual Clauses

1. *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 organisation:	The data exporter is the legal entity specified as "Customer" in the DPA.
Address:	As indicated in the Agreement.
Tel:	Contact details for the data exporter are specified in the Agreement.
Fax:	
E-mail:	Contact details for the data exporter are specified in the Agreement.
Other information needed to identify the organisation	....

(**the data exporter**)

And

Name of the data importing organisation:	insightsoftware
address:	8529 Six Forks Road, Suite 400 Raleigh, NC 27615, United States of America
Tel:	(919) 872-7800
Fax:	
E-mail:	privacy@insightsoftware.com
Other information needed to identify the organisation	....

(**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 Annex A.

2. Definitions

For the purposes of the Clauses:

(a) personal data, special categories of data, process/processing, controller, processor, data subject and Commissioner shall have the same meaning as in the UK GDPR

(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 covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 its 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 UK;

(f) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

3. *Details of the transfer*

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

4. *Third-party beneficiary clause*

4.1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to Clause 4(i), Clause 5(a) to Clause 5(e) and Clause 5(g) to Clause 5(j), Clause 7.1 and Clause 7.2, Clause 7, Clause 8.2 and Clause 9 to Clause 12 as third-party beneficiary.

4.2. The data subject can enforce against the data importer this Clause, Clause 5(a) to Clause 5(e) and Clause 5(g), Clause 6, Clause 7, Clause 8.2 and Clause 9 to Clause 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.

4.3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to Clause 5(e) and Clause 5(g), Clause 6, Clause 7, Clause 8.2 and Clause 9 to Clause 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 sub-processor shall be limited to its own processing operations under the Clauses.

4.4. 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.

5. Obligations of the data exporter

The data exporter agrees and warrants:

(g) 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 Commissioner) and does not violate the applicable data protection law;

(h) 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;

(i) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex B to this contract;

(j) 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, unauthorised 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;

(k) that it will ensure compliance with the security measures;

(l) 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 covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(m) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(n) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex B and a summary description of the security measures, as well as a copy of any contract for sub-processing 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;

(o) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(p) that it will ensure compliance with Clause 4(a) to Clause 4(i).

6. *Obligations of the data importer*

The data importer agrees and warrants:

(q) 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;

(r) 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;

(s) that it has implemented the technical and organisational security measures specified in Annex B before processing the personal data transferred;

(t) 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 unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(u) 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 Commissioner with regard to the processing of the data transferred;

(v) 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 Commissioner;

(w) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(x) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(y) that the processing services by the sub-processor will be carried out in accordance with Clause 11; and

(z) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

7. Liability

7.1. 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

7.2. 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 its sub-processor 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.

7.3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

7.4. 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

8. Mediation and jurisdiction

8.1. 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:

(aa) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

(bb) to refer the dispute to the UK courts.

8.2. 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.

9. Cooperation with supervisory authorities

9.1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

9.2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, 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.

9.3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

10. Governing Law

10.1. The Clauses shall be governed by the laws of England and Wales.

11. Variation of the contract

11.1. The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

12. Sub-processing

12.1. 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[5]. Where the sub-processor 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 sub-processor's obligations under such agreement.

[5] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

12.2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

12.3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of England and Wales.

12.4. The data exporter shall keep a list of sub-processing 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 Commissioner.

13. Obligation after the termination of personal data processing services

13.1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor 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.

13.2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

ANNEX A to the UK Standard Contractual Clauses of Attachment B

This Annex forms part of the Clauses and must be completed and signed by the parties.

Data exporter

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

The Customer who purchased Services from insightsoftware

Data importer

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

insightsoftware, who provides Services to the Customer and the performance of insightsoftware's obligations under the Agreement and this DPA or as otherwise agreed by the Parties

Data subjects

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

May include:

- Users of the insightsoftware Software, Support Services, and/or Cloud Services (as defined in the Agreement);
- Employees, contractors and other agents of insightsoftware's customers;
- Suppliers; and
- With respect to Certent Equity Management software applications and services: Shareholders, former employees, and other equity participants.

Categories of data

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

Data derived from use of the insightsoftware Software, Services, or Cloud Services may include:

- Customer user details, which may include:
  - Name and surname;
  - Title and position;
  - Business email address; and
  - Business phone number.
- IT management and security details, which may include:
  - Connection data;
  - Log-in credentials: user name and passwords; and
  - IP address.
- Financial and transactional details, which may include:
  - Income;
  - Benefits;
  - Brokerage information;

    - Assets and investments; and
    - Bank account number.
- Human resources and employment details, which may include:
    - Social security number;
    - TaxID;
    - Trust information;
    - Home physical address;
    - Personal email address; and
    - Personal phone number.
- Other, which may include miscellaneous data uploaded to the Software, Services, or Cloud Services by Customer's users.

Special categories of data (if appropriate)

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

In the normal, intended use case of the insightsoftware Software, Services, and Cloud Services, special categories of data should not be provided.

Processing operations

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

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction of data, pursuant to the instructions of the data exporter.

DATA EXPORTER

Name:...

Authorised signature:...........................

DATA IMPORTER

Name:..............David Woodworth..............

Authorised signature:.........................

DocuSigned by:

David Woodworth

DFF00F65033B4B9...

Annex B to the UK Standard Contractual Clauses of Attachment B

This Annex B forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clause 4(d) and Clause 5(c) (or documents/legislation attached):

Please see Attachment C for the insightsoftware Security Provisions

Attachment C

insightsoftware Security Provisions

insightsoftware implements the following technical and organizational security measures to protect personal data and relevant operational processes.

1. **insightsoftware Corporate Security Controls.**

   a. **Administrative Controls.**

      i. **Dedicated Information Security Team.** insightsoftware's Security Program is managed by a dedicated team of information security professionals, led by the insightsoftware VP and Chief Information Security Officer.

      ii. **Security Policy**. insightsoftware maintains a written security policy based on industry standards and in compliance with applicable data protection laws ("Data Protection Laws"), which is reviewed and updated annually and made available to all insightsoftware personnel.

      iii. **Background Checks**. insightsoftware conducts criminal background screening on its employees as part of its hiring process in compliance with applicable laws. Background checks are provided for all employees in some countries and, in other countries, are available to be performed upon request.

      iv. **Security Awareness Training.** insightsoftware maintains a documented security awareness training program for its personnel, including new hire and on-going training.

      v. **Code of Conduct; Confidentiality Agreements; Information Security Policy**. insightsoftware personnel are required to acknowledge and agree to several policies and agreements that require employees to maintain the confidentiality of Customer Data and follow security processes related to Customer Data, including the insightsoftware Code of Conduct, employee confidentiality agreements and the insightsoftware Information Security Policy.

      vi. **insightsoftware Risk Management & Threat Assessment.** insightsoftware has a documented risk management process. insightsoftware's Information Security Committee meets regularly to review reports and material changes in the threat environment, identify potential control deficiencies and make recommendations for new or improved controls and threat mitigation strategies.

      vii. **External Threat Intelligence Monitoring.** insightsoftware reviews external threat intelligence feeds, including US-Cert vulnerability announcements, critical vendor security advisories and other trusted sources of vulnerability and threat information.

      viii. **Vendor Risk Management.** insightsoftware evaluates vendors that process Customer Data or are part of an insightsoftware solution, to ensure they maintain security measures consistent with insightsoftware's obligations in this Security Addendum and in compliance with Data Protection Laws.

   b. **Incident Detection and Response.**

      i. **Incident Response Plan.** insightsoftware maintains a documented incident response plan, which includes incident reporting, response, roles and responsibilities, prioritization, escalation and remediation. The plan is tested and updated periodically.

      ii. **Security Incident Reporting.** If insightsoftware becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Security Incident"), insightsoftware shall notify Customer without undue delay, and in any case, within 48 hours after determining a Security Incident has impacted or will impact the Customer Data.

      iii. **Investigation.** In the event of a Security Incident, insightsoftware shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

      iv. **Communication and Collaboration.** insightsoftware shall provide Customer timely information about the Security Incident to the extent known to insightsoftware, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by insightsoftware to mitigate or contain the Security Incident, the status of insightsoftware's investigation, and a contact point to obtain additional information.

- **v.** **Cyber Insurance.** insightsoftware maintains a Cyber/Technology Errors & Omissions Liability insurance policy with a Policy Holder Alphabetic Category Rating of not less than "A-" and Financial Size Category Rating of not less than "VII" according to the latest edition of A.M. Best's Key Rating Guide.

c. **insightsoftware Corporate Office Physical & Environmental Controls.** insightsoftware's technical, administrative, and physical controls for its corporate offices covered by its ISO 27001 certification include, but are not limited to:

- **i.** Physical access to the corporate office is controlled at ingress points;
- **ii.** Badge access is required for all personnel and badge privileges are reviewed regularly;
- **iii.** Visitors are required to sign in;
- **iv.** CCTV covers building ingress points;
- **v.** Fire detection and protection systems; and
- **vi.** Climate control systems.

d. **insightsoftware System Security.**

- **i.** **Malware and Vulnerability Protection.** insightsoftware laptops, desktops and production servers are protected with auto-updating anti-malware protection and vulnerability monitoring. Email, including links and attachments in emails, are scanned for malware before being delivered.
- **ii.** **Disk Encryption.** insightsoftware laptop hard drives are encrypted.
- **iii.** **Patching.** Security patches are reviewed and deployed at least monthly.
- **iv.** **Secure Disposal.** insightsoftware follows a documented process for the secure deposal of assets which store data.
- **v.** **Multi-factor Authentication**. Remote access to insightsoftware networks require multi-factor authentication.

e. **Secure Software Development.**

- **i.** Security is part of the entire software development lifecycle.
- **ii.** Development systems are separate from production systems.
- **iii.** Customer Data is not transmitted to or stored on development systems.
- **iv.** Application security testing is built into the software development pipeline.
- **v.** A source code control system is utilized that authenticates and logs the person associated with all changes to the software or custom code baseline and all related configuration and build files.
- **vi.** Source code is backed up and protected.

2. **Cloud Security Controls and Safeguards.**

a. **Security Responsibilities.** insightsoftware provides its software either (i) on an on-premise basis, whereby the software is installed on Customer's computers, or (ii) as a hosted service, whereby insightsoftware utilizes infrastructure-as-a-service cloud providers and/or secure colocation facilities to provide Customers access to the insightsoftware software (the "Cloud Environment"). With respect to insightsoftware's on-premises software, which is installed on Customer's computers, the Customer is responsible for maintaining the security of Customer's computers, including all patching, access controls, firewalls, physical security, backups and encryption. When insightsoftware's software is provided via a Cloud Environment, insightsoftware is responsible for maintaining the security controls and safeguards described below. insightsoftware maintains a comprehensive documented security program under which insightsoftware implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the software and Customer Data.

b. **insightsoftware's Audits and Certifications.**

- **i.** insightsoftware maintains the audits and certifications described at https://legal.insightsoftware.com/contracts/ISO&SOC-certifications.pdf.
- **ii.** Reports by independent third-party auditors are made available to Customer upon request.

c. **Hosting Location of Customer Data.** insightsoftware uses subservice organizations whose controls are assessed via SOC 2 audits to ensure they are suitably designed and operated to comply with insightsoftware's security requirements.

d. **Encryption.**

   i. **Encryption at Rest**. Customer data residing in the Cloud Environment are encrypted at rest.

   ii. **Encryption Key Management.** All cryptographic keys are protected from unauthorized disclosure or use.

      1. Encryption keys are created in compliance with the then current industry standard strength recommendations.
      2. Any key that becomes weak due to outdated algorithms or is suspected of compromise is retired and/or rotated with an updated key.
      3. Certificates are utilized to encrypt keys used to encrypt data.

   iii. **Encryption in transit.** Secure data transmission protocols are used to encrypt confidential data when transmitted over public networks.

e. **System and Network Security.**

   i. **Access Controls.** All insightsoftware personnel access to the Cloud Environment is via a unique user ID with a complex password and multi-factor authentication. Access to systems and data is provided to individuals when required to perform their job functions and is consistent with the principle of least privilege.

   ii. **Separation of Environments.** insightsoftware logically separates production environments from development and testing environments. The Cloud Environment is both logically and physically separate from insightsoftware's corporate offices and networks.

   iii. **Change Management.** insightsoftware maintains a documented change management program for its software.

   iv. **Firewalls/Security Groups.** insightsoftware's Cloud Environment uses industry standard firewall or security groups technology with deny-all default policies to permit only business-required network traffic protocols and to protect systems from untrusted networks.

   v. **Personnel Access Reviews & Separation.** insightsoftware reviews the access privileges of its personnel to the Cloud Environment at least quarterly and removes access on a timely basis for all separated personnel.

   vi. **Hardening.** The Cloud Environment is hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

   vii. **Patching.** Security patches are reviewed and applied to systems on a regular basis in accordance with established policies and standards.

   viii. **Monitoring & Logging.** Monitoring tools and services are utilized to log specific activities and changes within the Cloud Environment. These logs are further monitored and analyzed for anomalies when necessary. The logs are securely stored to prevent tampering.

   ix. **Endpoint Protection**. The Cloud Environment leverages auto-updating threat detection tools to monitor for and provide protection from suspicious activities and malware (collectively, "Malicious Activity") on in-scope endpoints. insightsoftware does not monitor Customer Data for Malicious Activity.

   x. **Vulnerability Management.** Systems in the Cloud Environment are automatically evaluated for vulnerabilities, which are then prioritized for remediation based on their potential impact to insightsoftware's software.

   xi. **Penetration Testing**. insightsoftware engages one or more independent third parties to conduct penetration tests of selected software at least annually. Upon Customer's written request, insightsoftware shall provide Customer an executive summary of any such penetration test.

f. **Cloud Data Center Physical & Environmental Controls.** To ensure the Cloud Environment has appropriate physical and environmental controls for the data centers hosting the software, insightsoftware regularly reviews Cloud Environment security controls audited under by independent third-party audits and certifications. Each Cloud Environment provider has a SOC 2 Type II annual audit and ISO 27001 certification, or industry-recognized equivalent framework. Such controls include, but are not limited to, the following:

- **i.** Physical access to the facilities and physical systems is controlled;
- **ii.** Physical access privileges are reviewed regularly;
- **iii.** Visitors are required to present ID and sign in;
- **iv.** CCTV covers all ingress points;
- **v.** Fire detection and protection systems;
- **vi.** Power back-up and redundancy systems;
- **vii.** Climate control systems; and
- **viii.** Established NIST 800-88 compliant processes for decommissioning hardware assets.

g. **Deletion of Customer Data by insightsoftware.** Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement, insightsoftware promptly deletes any remaining Customer Data.

h. **Business Continuity and Disaster Recovery.** Automated backup systems perform scheduled backups of production databases. For the software for which insightsoftware maintains audits, a business continuity and disaster recovery plan is in place to ensure the resumption of time-sensitive operations and services in the event of a disastrous event that causes a significant business interruption. The business continuity and disaster recovery plan contains detailed responsibilities and specific tasks for emergency response activities and business resumption operations based upon pre-defined time frames. The plan is reviewed and tested on an annual basis to validate that documented procedures are appropriate and to ensure that personnel understand the plan and the role that they play in executing the plan.

3. **Customer Audit Rights.** Upon written request and at no additional cost to Customer, insightsoftware shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing insightsoftware's compliance with its obligations under this Security Addendum in the form of, as applicable, (i) insightsoftware's ISO 27001 certification, (ii) insightsoftware's SOC 2 Type II audit report and/or SOC 1 Type II audit report, (iii) insightsoftware's most recently completed Shared Assessments Standardized Information Gathering (SIG) Questionnaire, and (iv) the most recent penetration test summary report for the relevant Software ("**Audit Reports**"). In the event insightsoftware is unable to provide an Audit Report, insightsoftware agrees to complete any Customer-provided information security questionnaire on an annual basis within six (6) weeks of Customer's written request. Where the Auditor is a third-party, such third party may be required to execute a separate confidentiality agreement with insightsoftware prior to any review of Audit Reports, and insightsoftware may object in writing to such third party if in insightsoftware's reasonable opinion the third party is not suitably qualified or is a direct competitor of insightsoftware. Any such reasonable objection by insightsoftware will require Customer to appoint another third party. Any expenses incurred by an Auditor in connection with any review of Audit Reports, or a customer-provided questionnaire shall be borne exclusively by the Auditor.