

Insightly, Inc. Data Processing Addendum

1. Introduction

This Data Processing Addendum (“**Addendum**”) is an integral part of the Insightly Terms of Service (the “**Terms**”), the Professional Services Agreement (if any) , and Privacy Policy which together with any exhibits, form the “**Agreement**” between Insightly, Inc. (“**Insightly**”) and the customer who entered into the Terms of Service (“**Customer**”). This Addendum governs the manner in which Insightly shall process Customer Personal Data (as defined below) and shall be effective as of the date both parties sign this Addendum. In the event of a conflict between the Agreement, including any exhibits, and this Addendum, the provision imposing the stricter data protection requirements of any conflicting provision shall control.

Capitalized terms have the meaning given to them in the Agreement, unless otherwise defined below.

2. Definitions

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

- a) “**Applicable Data Protection Law(s)**” means the relevant data protection and data privacy laws, rules and regulations to which the Customer Personal Data are subject. “Applicable Data Protection Law(s)” shall include, but not be limited to, the California Consumer Privacy Act of 2018 (“**CCPA**”) and EU General Data Protection Regulation (2016/679) (the “**GDPR**”).
- b) “**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal data.
- c) “**Customer Personal Data**” means Personal Data pertaining to Customer’s users or employees located in the European Union and received or collected by Insightly. The Customer Personal Data and the specific uses of the Customer Personal Data are detailed in Schedule 1, as required by the GDPR.
- d) “**Personal Data**” shall have the meaning assigned to the terms “personal data” or “personal information” under Applicable Data Protection Law(s).
- e) “**Process**,” “**Processes**,” “**Processing**,” “**Processed**” means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- f) “**Processor**” means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data subject to this Addendum.
- g) “**Security Incident(s)**” means the unauthorized access, use or disclosure of Customer Personal Data.
- h) “**Third Party(ies)**” means Insightly authorized contractors, agents, vendors and third party service providers (i.e., sub-processors) that Process Customer Personal Data.

3. Data Handling and Access

- a) General Compliance. Customer Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).
- b) Insightly and Third Party Compliance. Insightly agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties’ Processing of Customer Personal Data that imposes on such Third Parties data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Insightly’s Third Parties’ (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.
- c) Authorization to Use Third Parties. To the extent necessary to fulfill Insightly’s contractual obligations under the Agreement or any Statement of Work, Customer hereby authorizes (i) Insightly to engage Third Parties and (ii) Third Parties to engage sub-processors. Any transfer of

Customer Personal Data shall comply with all Applicable Data Protection Law(s). Insightly will provide Customer any records of Processing of Customer Personal Data that Processors are required to maintain and provide under Applicable Data Protection Law(s).

- d) Right to Object to Third Parties. Insightly shall include a list of approved Third Parties as of the effective date of this Addendum in Schedule 2. Thereafter, upon request, Insightly shall make available to customer an updated list of Third Parties. Customer may object to any new Third Party within thirty (30) days of receipt of the updated list, such that Insightly will either (a) instruct the Third Party to cease any further processing of Customer Personal Data, in which event this Addendum shall continue unaffected, or (b) allow Customer to terminate the part of the service performed under the Agreement that cannot be performed by Insightly without use of the objectionable Third Party. If Customer does not object, the new Third Party shall be deemed accepted and Insightly may continue to use it.
- e) Following Instructions. Insightly shall Process Customer Confidential Data only in accordance with the written instructions of Customer or as specifically authorized by this Addendum, or the Agreement. Insightly will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions.
- f) Confidentiality. Any person authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.
- g) Personal Data Inquiries and Requests. Insightly agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Personal Data granted to them under Applicable Data Protection Law(s) ("**Privacy Request**"). At Customer's request and without undue delay, Insightly agrees to assist Customer in answering or complying with any Privacy Request.
- h) [Limitation on Disclosure of Customer Personal Data. To the extent legally permitted, Insightly shall: (i) promptly notify Customer's Designated POC in writing upon receipt of an order, demand, or document purporting to request, demand or compel the production of Customer Personal Data to any third party, including, but not limited to the United States government for surveillance and/or other purposes; and (ii) not disclose Customer Personal Data to the third party without providing Customer at least forty-eight (48) hours' notice, so that Customer may, at its own expense, exercise such rights as it may have under applicable laws to prevent or limit such disclosure.]

4. EU - U.S. Compliance

- a) Cross-Border Data Transfer Mechanism. Customer will operate as a data Controller and Insightly will operate as a data Processor Processing Customer Personal Data only as necessary for the limited and specified purposes identified in this Addendum and/or the Agreement. Customer authorizes Insightly and its Third Parties to transfer Customer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.
- b) Standard Contractual Clauses. If Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Insightly in a country that has not been found to provide an adequate level of protection under Data Protection Laws, the parties agree that the terms of the transfer shall be governed by the Standard Contractual Clauses attached hereto as **Exhibit A**. The parties agree that: (i) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Section 7 of this Addendum; (ii) pursuant to Clause 5(h) and Clause 11 of the Standard Contractual Clauses, Insightly may engage new Subprocessors in accordance with Section 3(b) – (d) of this Addendum; and (iii) the Subprocessor agreements referenced in Clause 5(j) and certification of deletion referenced in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Customer's written request. Each party's signature to the Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.
- c) Prior Consultation. Insightly agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's judgement, the type of Processing performed by Insightly is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large

scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

- d) Demonstrable Compliance. Insightly agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide such records to Customer upon reasonable request to assist Customer with complying with supervisory authorities' requests.
- e) Notice of Non-Compliance. Insightly shall promptly notify Customer if it can no longer meet its obligations under this Section 4.

5. Information Security Program

Insightly agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s) (the "**Information Security Program**"). Further, Insightly agrees to regularly test, assess and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing.

6. Audits

Upon request from Customer and at Customer's expense, Insightly agrees to reasonably cooperate with Customer for the purpose of verifying Insightly's compliance with Applicable Data Protection Law(s).

7. Data Retention and Deletion upon Termination


Upon termination of the Agreement, Customer will be able to (with Insightly's assistance if needed) delete the Customer Personal Data in Insightly's possession or control by removing all Customer Personal Data from the Insightly Service and deleting its account. At Customer's discretion, either directly, or with the assistance of Insightly, Customer shall have the opportunity to first export all Customer Personal Data before deleting its account. The foregoing requirement will not apply to the extent Insightly is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data that is archived on Insightly's back-up systems. With regards to such Customer Personal Data on Insightly's back-up systems, Insightly will stop Processing and destroy or deidentify such data according to its data retention policies, except to the extent required by applicable law.

8. Security Incident

- a) Security Incident Procedure. Insightly will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.
- b) Notice. Insightly agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) to Customer if a known Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

IN WITNESS WHEREOF, the parties have caused this Addendum to be signed by their duly authorized representatives.

Company: _____
Signature: _____
Name: _____
Title: _____
Date: _____

INSIGHTLY, INC : 
Signature: _____
Name: Mohit Kukreja
Title: VP, Engineering
Date: 08/31/2020

Schedule 1 to the Insightly Data Processing Addendum

1.1 Subject Matter of Processing	The subject matter of Processing is the Insightly Service pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	<p>Includes the following :</p> <ul style="list-style-type: none"> ● With respect to Personal Data stored by Customer using the Insightly Service: <ul style="list-style-type: none"> - Any type of category of Data Subjects stored at the discretion of Customer as allowed under the Agreement ● With respect to Customer's authorized users of the Insightly Service, categories of Data Subjects include: <ul style="list-style-type: none"> - Employees, agents, advisors, partners (any category of authorized users) - Any category of Data Subjects stored at the discretion of Customer which may be conveyed via a support request by Customer
1.4 Nature and Purpose of Processing	The purpose of Processing of Customer Personal Data by Insightly is the performance of the Insightly Service pursuant to the Agreement.
1.5 Types of Personal Data	<p>Includes the following:</p> <ul style="list-style-type: none"> ● With respect to Personal Data stored by Customer using the Insightly Service: <ul style="list-style-type: none"> - Any type of Personal Data stored at the discretion of Customer as allowed under the Agreement ● With respect to Customer's authorized users of the Insightly Service, Personal Data may include: <ul style="list-style-type: none"> - Authorized user identification data (notably account name, user name, payment information, email address. Also may include address and telephone number) - Any type of Personal Data stored at the discretion of Customer which may be conveyed via a support request by Customer as allowed under the Agreement

Schedule 2 to the Insightly Data Processing Addendum

Third Parties as of the effective date of this Addendum:

Third Parties of the Insightly Service which may Process Customer Personal Data on behalf of Insightly:

1. Google Inc
2. Amazon Web Services
3. Stripe
4. Recurly
5. ProfitWell
6. Pendo
7. Zendesk
8. Raygun
9. Papertrail
10. Salesloft
11. Drift
12. Zoom
13. SendGrid
14. New Relic
15. SnowPlow
16. Twilio
17. Talkdesk
18. CloudApp

Exhibit A

Standard Contractual Clauses (Processors)

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: Customer (as defined in the Addendum).

(the data **exporter**)

And

Name of the data importing organisation: Insightly (as defined in the Addendum).

(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 Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and 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.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, 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;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or 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;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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

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

Clause 7

Mediation and jurisdiction

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

Clause 8

Cooperation with supervisory authorities

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

Clause 9
Governing Law

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

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

Data exporter

The data exporter is: Customer.

Data importer

The data importer is: Insightly.

Data subjects

The personal data transferred concern the following categories of data subjects: As set forth in Schedule 1 of the Addendum.

Categories of data

The personal data transferred concern the following categories of data: As set forth in Schedule 1 of the Addendum.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: As set forth in Schedule 1 of the Addendum.

Processing operations

The personal data transferred will be subject to the following basic processing activities: Processing to carry out the Services pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 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 Clauses 4(d) and 5(c):

Insightly will use commercially reasonable efforts to implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data in accordance with the Addendum.