INSPECTIV, INC.

Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements and is incorporated by this reference into the Terms of Service Agreement entered into between Inspectiv, Inc. ("**Inspectiv**") and the Customer (the "**Agreement**"). This DPA only applies to the extent that Inspectiv actually Processes Personal Data in providing the Services. Personal Data is not intended to be in scope for the Services, but may be incidentally accessed if a security vulnerability exposes such data.

Data Protection Laws worldwide place certain obligations upon a Controller, to ensure that a Processor engaged by the Controller provides sufficient guarantees that any such Processing is secure. This DPA exists to ensure that there are sufficient security measures in place and that the Processing complies with the Parties' obligations under such Data Protection Laws. Except as expressly set forth in this DPA, all other terms and conditions of the Agreement will continue and remain in full force and effect. In the event of a conflict between the Agreement and this DPA, the provision imposing the stricter data protection requirements of any conflicting provision will control. Capitalized terms will have the meaning given to them in the Agreement, unless otherwise defined below.

1. **Definitions** Any capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement.

a. "**CCPA**" means Title 1.81.5, California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended by Proposition 24, the California Privacy Rights Act of 2020 ("**CPRA**"). The CCPA is a data privacy law that provides California consumers with a number of privacy protections, including the right to access, delete and opt-out of the "sale" or "sharing" of their Personal Data (as such terms are defined in the CCPA).

b. "**Applicable U.S. Privacy Laws**" means any U.S. state consumer data privacy law applicable to the Processing of Personal Data under this DPA, including without limitation the CCPA (as defined herein), and the comprehensive consumer privacy laws of any other U.S. state in which data subjects whose Personal Data is Processed under this DPA reside, in each case as amended or supplemented from time to time. Where this DPA references obligations under the CCPA or any Applicable U.S. Privacy Law, Inspectiv will comply with such obligations to the extent, and only to the extent, that such law applies to the Personal Data being Processed.

c. "**Controller**" means an entity which, alone or jointly with others, determines the purposes and means of Processing of Personal Data (including as applicable, a "business" as defined by the CCPA).

d. "**EU Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 ("**GDPR**") and any national implementing legislation of EU Member States in relation to data protection.

e. "**EU Standard Contractual Clauses**", "**SCCs**" or "**Clauses**" means, where the EU Data Protection Laws apply, the Standard Contractual Clauses forming part of Decision 2021/914/EC (as amended or replaced from time to time), including their appendices and with the relevant Modules and Options set out herein.

f. "**Personal Data**" means any information that constitutes "personal data" or "personal information" within the meaning of applicable data protection laws that forms part of Customer's data and that Inspectiv intentionally receives from Customer or incidentally accesses by or on behalf of Customer in connection with the Agreement.

g. "**Processor**" means an entity which Processes Personal Data on behalf of the Controller (including as applicable, a "service provider" as defined by the CCPA).

h. "**Sub-processor**" means a third-party service provider engaged by Inspectiv to assist with the Processing of Personal Data.

i. "**UK Data Protection Laws**" means the Data Protection Act 2018 and the United Kingdom's version of the GDPR which is part of UK law by virtue of the European Union (Withdrawal) Act 2018 ("**UK GDPR"**) and any legislation applicable in the UK in force from time to time relating to privacy or the Processing of Personal Data.

j. "**UK Standard Contractual Clauses**" means, where the UK Data Protection Laws apply, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, as currently set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, and as revised under Section 18 of the International Data Transfer Addendum (the "**UK Addendum**").

2. **Roles, Limitations on Use**

a. The Parties acknowledge and agree that regarding Personal Data, Customer may be a Controller or a Processor acting on its client's behalf. Where Customer is a Controller, if any only to the extent that Inspectiv Processes Personal Data, Inspectiv will be a Processor; and where Customer is a Processor, Inspectiv will be a Sub-processor. To the extent that Inspectiv also provides Services to, and Processes Personal Data provided by or on behalf of an Affiliate of Customer, each such Affiliate will be the Controller of the Personal Data that it provides to Inspectiv and such Affiliate will have the same rights that Customer has under this DPA when such Affiliate is a Controller in respect of the Personal Data.

b. As the Processor (or as applicable, Sub-processor), Inspectiv will Process Personal Data solely in accordance with (i) the Agreement or other documented instructions of Customer (whether in written or electronic form) provided in accordance with the Agreement or (ii) as otherwise required by applicable Laws, in which case Inspectiv will inform Customer of the legal requirement before Processing, unless legally prohibited on grounds of public interest. Customer acknowledges and agrees that Customer's final and complete instructions regarding the Processing of Personal Data are set out in the Agreement. Any additional or alternate instructions must be agreed in writing by the Parties (and Inspectiv will be entitled to charge a reasonable Fee to cover any compliance costs incurred).

c. Inspectiv will ensure that persons authorized to Process Personal Data on Inspectiv's behalf have committed themselves to confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

d. As the Controller, Customer is responsible for ensuring that, in accordance with Data Protection Laws, (i) there is a lawful basis for the collection and Processing of Personal Data and (ii) Customer has provided an appropriate privacy policy to its Authorized Users and other data subjects.

e. The Parties acknowledge and agree that regarding Usage Metadata, Inspectiv is an independent Controller, not a joint Controller with Customer. Inspectiv will process Usage Metadata as a Controller: (i) to manage the relationship with Customer; (ii) to carry out Inspectiv's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, Security Incidents and other misuse of the Services or other Inspectiv Technology, and to prevent harm to Customer; (iv) for purposes of identity verification; (v) to comply with legal or regulatory obligations applicable to the Processing and retention of Personal Data to which Inspectiv is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Inspectiv may also process Usage Metadata as a Controller in order to provide, optimize, and maintain the Services or other Inspectiv Technology, to the extent permitted by Data Protection Laws. Any processing by Inspectiv as a Controller will be in accordance with (A) applicable Data Protection Laws and (B) Inspectiv's Privacy Policy set forth at https://www.inspectiv.com/legal/privacy-policy.

3. **Sub-processors** Customer agrees that Inspectiv may disclose Personal Data to its Sub-processors for purposes of providing the Services to Customer, provided that Inspectiv will impose on its Sub-processors data protection obligations that are at least as protective of Personal Data as those set forth in this DPA. Inspectiv has made available to Customer a list of its Sub-processors as Schedule 1 hereto, which Sub-processors have been approved by Customer via the Agreement or this DPA. Inspectiv will provide

Customer with a mechanism to receive notice of any changes to this list. Inspectiv will notify Customer of the addition of any new Sub-processors by updating this list at least 30 days before granting the new Sub-processor access to Customer Personal Data, in order to allow Customer an opportunity to object to the addition. Inspectiv will be liable for the acts or omissions of any Sub-processors to the same extent as if the acts or omissions were performed by Inspectiv. Inspectiv will disclose Personal Data only to approved Sub-processors or as otherwise expressly authorized under the Agreement or this DPA or as required by applicable Laws.

4. **Data Transfers** In providing the Services, and unless expressly agreed otherwise in writing by the Parties, Inspectiv and its Sub-processors may transfer Personal Data to other countries where they have operations, or as otherwise required by applicable Laws. Inspectiv will implement appropriate measures to protect Personal Data in accordance with this DPA and in compliance with applicable Data Protection Laws, regardless of the jurisdiction in which it is located. Any cross-border transfers of Personal Data will take place only where enforceable data subject rights and effective legal remedies for data subjects are available and appropriate safeguards are in place in relation to the transfer, as provided for by: (a) the SCCs as referenced herein; or (b) any other data transfer mechanisms permitted by Data Protection Laws, as appropriate.

5. **Security** Inspectiv will implement reasonable technical and organizational safeguards designed to protect Personal Data against unauthorized loss, destruction, alteration, access, or disclosure. Inspectiv will require Inspectiv personnel who will be provided access to, or will otherwise Process, Personal Data, to protect Personal Data consistent with the standards set forth in this DPA. If Inspectiv discovers a Security Incident has occurred, Inspectiv will notify Customer without undue delay and, in any event, within 24 hours of becoming aware of such Security Incident (or such timeframe as required by applicable Data Protection Laws). Such notification will include, to the extent then known: (a) the nature of the Security Incident, including the categories and approximate number of data subjects and Personal Data records affected; (b) the likely consequences of the Security Incident; and (c) the measures taken or proposed to address the Security Incident, including to mitigate its possible adverse effects. Inspectiv will provide Customer with such further information and assistance as Customer may reasonably require in connection with any notification obligations Customer may have under applicable Data Protection Laws.

6. **Audit** Upon Customer's written request and as applicable, execution of a Inspectiv standard nondisclosure agreement, Inspectiv will provide responses up to once per year to any written questions that Customer may reasonably submit for purposes of verifying Inspectiv's compliance with this DPA. If Customer reasonably determines that further assessment is required by applicable Laws, then Customer at its sole expense and upon reasonable advance written notice may perform a review, once per year during the term (other than where a Security Incident has taken place, in which case Customer will be entitled to carry out an additional review within 30 days of Inspectiv notifying Customer of such Security Incident), of the relevant policies, procedures and related documentation of Inspectiv's Services. The timing, scope and duration of any such review will be mutually agreed by the Parties. Any such review will be conducted in a manner that does not compromise confidentiality obligations to any of Inspectiv's other clients or other third parties. Customer will ensure that any third-party auditor that Customer appoints in connection with a review is: (a) not a Inspectiv competitor; and (b) is committed to appropriate confidentiality obligations. Customer and/or any third-party auditor will comply with Inspectiv's standard policies and procedures when accessing Inspectiv's premises or systems.

7. **Individual Requests or Complaints** Inspectiv will promptly notify Customer, unless prohibited by applicable Laws, if Inspectiv receives: (a) any request from an individual with respect to Personal Data Processed by Inspectiv, including but not limited to opt-out requests, requests for access, rectification and/or correction, blocking, erasure, requests for data portability and all similar requests; or (b) any complaint relating to the Processing by Inspectiv of Personal Data, including allegations that such Processing infringes on a data subject's rights. Customer is responsible for responding to such requests and complaints from individuals and Inspectiv will provide such information and assistance as Customer may reasonably require in order to allow Customer to comply with its obligations under Data Protection Laws in regard to such requests.

8. **Return or Deletion** Upon termination or expiration of the Agreement, Customer will be entitled to retrieve its Personal Data in accordance with the Agreement; provided that, Customer must notify Inspectiv of Personal Data that Customer wishes to have returned or deleted within 30 days after the effective date of termination or expiration. Inspectiv will delete Personal Data from the Services promptly following such retrieval period unless otherwise required by applicable Laws; provided that, Inspectiv will be entitled to retain Personal Data where required by Data Protection Laws or other applicable Laws, or where such data is required for Inspectiv's internal record keeping or where it is necessary for use in legal proceedings.

9. **EU International Transfers**

a. With respect to EU-U.S. transfers of Personal Data, Inspectiv (acting on its own behalf and as agent for each Inspectiv Affiliate) and Customer (acting on its own behalf and as agent for each of its Affiliates) each hereby agree to Process such Personal Data in compliance with the EU SCCs incorporating:

i. The general clauses (*Clauses 1-6*);

ii. Modules One (*Transfer Controller to Controller*), Two (*Transfer Controller to Processor*), and Four (*Transfer Processor to Controller*) as applicable and the relevant options as specified in the table set out in Section 10 herein; and

iii. With the Annexes populated as set out below:

b. Annex I of the EU SCCs (Details of Data Processing) will be pre-populated with the details set out in Section 11.01 herein; and

c. Annex II of the EU Standard Contractual Clauses (Security Measures) are described in Section 11.02 herein.

d. Before commencing any EU international transfer to or from a Sub-processor, Inspectiv will ensure enforceable data subject rights and effective legal remedies for data subjects are available and appropriate safeguards are in place in relation to the transfer, as provided for by: (i) entering into the EU SCCs with such Sub-processor, incorporating the general clauses (Clauses 1-6) and Module 3 (Transfer Processor to Processor); or (ii) any other data transfer mechanisms permitted by Data Protection Laws, as appropriate.

e. **EU SCCs: Modules and Options** As applicable, the Parties agree that the following modules and options of the EU SCCs are deemed to be incorporated:

Clause 7 (*Docking clause*)	Clause 7 will not be incorporated.
Clause 8 (*Data protection safeguards*)	Modules 1, 2 and 4.
Clause 9 (*Use of Sub-processors*)	Module 2, Option 2, and the specific time period will be as set out herein.
Clause 10 *(Data subject rights*)	Modules 1, 2 and 4.
Clause 11 (*Redress*)	Module 1 and 2, and the Option in Clause 11(a) will not be incorporated.
Clause 12 (*Liability*)	Modules 1, 2 and 4.
Clause 13 (*Supervision*)	Module 1 and 2, incorporating all paragraphs of Clause 13(a) as applicable.
Clause 14 (*Local laws and practices affecting*	Modules 1, 2 and 4.

compliance with the Clauses)	
Clause 15 (*Obligations of the Data Importer in case of access by public authorities*)	Modules 1, 2 and 4.
Clause 16 (*Non-compliance with the Clauses and termination*)	For Clause 16(d) the relevant parts for Modules 1, 2 and 4.
Clause 17 (*Governing law*)	Modules 1 and 2, Options 1 and 2 as applicable and the law inserted will be the laws of the EU Member State in which the data exporter is established, save that: (i) where such laws do not allow for third-party beneficiary rights; or (ii) the data exporter is not established in an EU Member State, the law will be the laws of Ireland. Module 4 and the law inserted will be the laws of the country stated in the governing law clause of the Agreement, save that where such law does not allow for third-party beneficiary rights, the law will be the laws of Ireland.
Clause 18 (*Choice of forum and jurisdiction*)	Modules 1 and 2 and the courts inserted will be the courts in the Member State referred to in Clause 17 (*Governing law*). Module 4 and the country inserted will be the country stated to have jurisdiction in the Agreement, save that where the laws of that country do not allow for third-party beneficiary rights, the country will be the law of Ireland.

f. **EU SCCs: Details of Data Processing, Security Measures** As applicable, the Parties agree that Annex I of the EU SCCs will be pre-populated with the following details:

List of Parties	**Data Exporter**: **Name**: the person or entity agreeing to these terms (i.e., the Customer). **Address**: per Customer's SOs and/or SOWs. **Contact person's name, position, contact details**: per Customer's SOs and/or SOWs. **Activities relevant to the data transferred under these Clauses**: per the Agreement. **Role (Controller/Processor)**: Controller (or as applicable, Processor). **Data Importer(s)**: **Name**: Inspectiv, Inc. (for itself and its Affiliates) **Address**: 10866 Washington Blvd # 1300, Culver City, CA 90232 **Contact person's name, position, contact details**: Chief Information Security Officer, security@inspectiv.com **Activities relevant to the data transferred under these Clauses**: The Data Importer provides the Platform available at www.inspectiv.com and

	https://client.inspectiv.com/ (the "**Website**"), as well as other Services, products, features, software and Inspectiv Technology (collectively, the "**Services**"). **Role (Controller/Processor)**: Processor (or as applicable, Sub-processor).
Description of Processing	**Categories of data subjects whose Personal Data is transferred**: The Platform requires the transfer and Processing of Personal Data about the following categories of data subjects: 1. Data exporter's administrators, for the purposes of managing the Agreement and use of the Platform. 2. Permitted users of the Services, for the purposes of facilitating their access to and use of the Platform. **Categories of Personal Data transferred**: The Platform facilitates the transfer and Processing of Personal Data uploaded, submitted or otherwise transmitted to the Platform by the Data Exporter or any third party using the Data Exporter's account. Such Personal Data includes without limitation: full name; email address. **Sensitive data transferred**: The Platform does not require the transfer or Processing of any special categories of data (as defined in Article 9(1) of the GDPR). The Data Exporter will not provide or make available such data to the Data Importer, except as expressly agreed in writing by the Parties. **The frequency of the data transfer**: Continuous unless otherwise specified in the Agreement. **Nature of the Processing**: The Platform facilitates the following Processing of Personal Data on behalf of (and on the instructions of) the Data Exporter: 1. Collection of Personal Data, as outlined above, for the purposes of delivering the Platform; 2. Secure storage of Personal Data with Data Importer's cloud hosting provider; 3. Retrieval of Personal Data upon the request of the Data Exporter or the applicable data subject; and 4. Destruction of Personal Data either at the request of the Data Exporter or upon the expiration or termination of the Agreement. As set out in the Agreement, the Data Importer does not Process Personal Data for any purposes other than those requested by the Data Exporter and outlined in the Agreement and Inspectiv's Privacy Policy. **Purpose(s) of the data transfer and further Processing**: The purpose of the transfer or Processing of Personal Data is for provision of the Platform and related Services, as more particularly set forth in the Agreement (and SOs or SOWs entered into thereunder). **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 of the Processing of Personal Data described herein under the Agreement is for the term of such Agreement (and SOs or SOWs entered into

	thereunder) as such term is defined therein, and not thereafter except if specifically instructed to do so by the Data Exporter. **For transfers to Sub-processors, also specify the subject matter, nature and duration of the Processing**: See Schedule 1 to this DPA.
Competent supervisory authority	Data Protection Commission, 21 Fitzwilliam Square, D02 RD28, Dublin 2, Ireland Tel: +353 76 110 4800 Email: info@dataprotection.ie Website: http://www.dataprotection.ie/

g. **EU SCCs: Security Measures** As applicable, the Parties agree that Annex II of the EU SCCs will be pre-populated with the following details:

Description of the technical and organizational measures implemented by the Data Importer (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:

1. **Personnel** Data Importer's personnel will not process Personal Data without authorization. Personnel are obligated to maintain the confidentiality of any Personal Data and this obligation continues even after their engagement ends.

2. **Technical and Organizational Measures** Data Importer maintains a written information security program that includes policies, procedures, and controls governing the processing of Personal Data in accordance with the terms of the Agreement and this Appendix. The Data Importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Personal Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

3. **Permitted Use and Disclosure** Subject to the requirements set forth in this Appendix, the Data Importer will not transfer, rent, barter, trade, sell, rent, loan, lease or otherwise Process Personal Data in any manner other than as permitted or required by the Agreement or as otherwise instructed by the Data Exporter.

4. **Background Checks and Training** The Data Importer conducts reasonable and appropriate background investigations on personnel in accordance with applicable laws and regulations. Personnel must pass the Data Importer's background checks prior to being assigned to positions in which they will, or in which the Data Importer reasonably expects them to, have access to Personal Data. The Data Importer conducts annual mandatory security awareness training to inform its personnel on relevant security procedures and the consequences of violating those procedures.

5. **Subcontractors** Any subcontractors: (a) are evaluated by the Data Importer to ensure that such subcontractors maintain appropriate physical, technical, organizational, and administrative controls consistent with the requirements of the Agreement and this Appendix. The Data Importer remains responsible for the acts and omissions of its subcontractors as if it had performed the acts or omissions itself and any subcontracting will not in any way reduce the Data Importer's obligations to the Data Exporter under the Agreement.

6. **Physical Security Measures** The Data Importer maintains appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that process Personal Data.

7. **Facility Access** Access to the Data Importer's facilities is tightly controlled. At termination of employment, the Data Importer promptly revokes terminated personnel's physical access to all corporate facilities.

8. **Access Controls** The Data Importer maintains a formal access control policy to control employee access to Personal Data. The Data Importer regularly reviews the access rights of authorized personnel and, upon change in scope of employment necessitating removal or employment termination, personnel access rights are removed.

9. **Separation** The Data Importer logically separates the Data Exporter's Personal Data from other customers' data.

10. **Continuity Plan** The Data Importer maintains a written business continuity and disaster recovery plan addressing the availability of Personal Data.

The Data Importer may update the above security measures from time to time upon written notice.

10. **UK International Transfers**

With respect to UK-U.S. transfers of Personal Data, Inspectiv (acting on its own behalf and as agent for each Inspectiv Affiliate) and Customer (acting on its own behalf and as agent for each of its Affiliates) each hereby agree to Process such Personal Data in compliance with the UK SCCs, i.e., the EU SCCs as implemented under this DPA, with the following modifications:

a. The EU SCCs will be deemed amended as specified by Part 2 of the UK Addendum;

b. Tables 1, 2 and 3 in Part 1 of the UK Addendum will be deemed completed respectively with the information set out in Section 11 of this DPA (as applicable); and

c. Table 4 in Part 1 of the UK Addendum will be deemed completed by selecting "importer" and "exporter.

11. Swiss International Transfers Regarding transfers of Personal Data from Switzerland to the United States or other third countries, Inspectiv (acting on its own behalf and as agent for each Inspectiv Affiliate) and Customer (acting on its own behalf and as agent for each Customer Affiliate) each hereby agree to Process such Personal Data in compliance with Switzerland's revised Federal Act on Data Protection ("**nFADP**"), which entered into force on September 1, 2023. To the extent that Personal Data transfers from Switzerland are not covered by an adequacy decision of the Swiss Federal Council, such transfers will be conducted pursuant to the EU SCCs as implemented under this DPA, with the following modifications required to address Swiss-specific requirements: (a) references to "Regulation (EU) 2016/679" will be construed as references to the nFADP; (b) references to "EU" or "Member State" will be construed to refer to Switzerland as applicable; (c) the competent supervisory authority will be the Swiss Federal Data Protection and Information Commissioner; and (d) the governing law of the SCCs as adapted herein will be the laws of Switzerland. Before commencing any international transfer of Personal Data from Switzerland to a Sub-processor, Inspectiv will ensure that appropriate safeguards are in place in relation to such transfer as required by the nFADP.

12. CCPA To the extent that Inspectiv Processes "Personal Information" subject to the CCPA:

a. Customer is a "Business" and Inspectiv is a "Service Provider", each as defined under the CCPA.

b. Inspectiv will not: (i) retain, use, disclose or otherwise Process "Personal Information" for any purpose, including a "Commercial Purpose", other than for the specific purposes as provided for in the Agreement or as needed to perform the Services, including to build or improve the quality of the Services,

to detect Security Incidents, to protect against fraudulent or illegal activity, to retain Sub-processors in compliance with this DPA, or as otherwise required or permitted by applicable Laws; (ii) "sell" or "share" Personal Information; (iii) Process Personal Information in any manner outside of the direct business relationship between Customer and Inspectiv; or (iv) combine Personal Information from Customer with Personal Information that Inspectiv received from or on behalf of another personal or entity or that Inspectiv collected from its own interactions with an individual.

c. Customer will only disclose Personal Information in connection with the Agreement, and only for the limited and specified purposes of receiving the Services.

d. Customer will not provide or make available to Inspectiv any "Sensitive Personal Information" (as defined under the CPRA) and/or personal health data, Personal Data of minors, PCI cardholder data or other sensitive data unless agreed by the Parties in writing. To the extent that Inspectiv does agree to Process Sensitive Personal Information on behalf of Customer, Inspectiv will Process such Sensitive Personal Information only for the specific purposes authorized by Customer in the Agreement, and will not use or disclose such Sensitive Personal Information for any other purpose, including without limitation to infer characteristics about a consumer, unless expressly permitted by applicable Law or the CPRA. Inspectiv will implement such additional technical and organizational safeguards as may be reasonably necessary to protect Sensitive Personal Information consistent with Customer's instructions and the requirements of the CPRA.

e. Upon written request from Customer, Inspectiv will provide written responses (which may include audit report summaries/extracts) to all reasonable requests for information made by Customer related to Inspectiv's Processing of Personal Information necessary to confirm Inspectiv's compliance with this DPA; provided that Customer will not exercise this right more than once in any 12-month rolling period. Notwithstanding the foregoing, Customer (or its appointed representatives) may also exercise such audit right of Inspectiv's operations and facilities if Customer is expressly requested or required to provide this information to a data protection authority, if Inspectiv has experienced a Security Incident, or as may be required under applicable Data Protection Laws. Such inspections will take place during normal business hours and will be subject to reasonable prior notice. In addition, upon written request from Customer, Inspectiv will provide documentation verifying that it no longer retains or uses any Personal Information that Customer has made a valid request to Inspectiv to cease using and/or delete. If, under the circumstances, the foregoing steps are insufficient (i) to ensure that Inspectiv uses the Personal Information collected pursuant to the Agreement in a manner consistent with Customer's obligations under the CCPA and this DPA or (ii) to stop and remediate Inspectiv's unauthorized use of Personal Information, then the Parties will promptly coordinate to determine any additional reasonable and appropriate steps that will be taken to ensure compliance. Inspectiv certifies that it understands the restrictions contained in this paragraph and will comply with them.

f. Each Party certifies that it understands the requirements under the CCPA.

g. As used in this Section 12, the following terms have the meanings set forth in the CCPA: (1) Personal Information; (2) Business; (3) Service Provider; (4) Commercial Purpose; (5) Sell; and (6) Share.

13. Automated Processing and Artificial Intelligence Customer acknowledges that Inspectiv may use AI-driven and autonomous systems in connection with the delivery of the Services, and the Parties agree as follows with respect to such processing:

a. Inspectiv will not Process Personal Data, Customer Materials or Customer Products to develop, train or fine-tune generalized machine-learning or AI systems. To the extent Inspectiv uses data to develop, train or fine-tune AI models that support security-analysis features within the Services, Inspectiv will use only anonymized, aggregated data for such purposes, such that no Personal Data is identifiable in connection therewith.

b. Inspectiv processes Services-related data (including vulnerability reports submitted by independent security researchers, scoping information and vulnerability-specific information and comments) using AI-driven and autonomous systems to enable and enhance delivery of the Services. These processes

include indexing, de-duplication and quality enhancement of vulnerability reports, enhanced search functionality and support workflows (collectively, "**AI-Assisted Processing**"). Such AI-Assisted Processing is performed in accordance with Customer's instructions and the terms of this DPA and the Agreement. To the extent any AI-Assisted Processing involves Personal Data, Inspectiv will perform such Processing subject to the same data protection obligations set forth in this DPA.

c. Inspectiv's AI-Assisted Processing does not involve solely automated decision-making (including profiling) that produces legal effects concerning, or similarly significantly affects, any data subject. To the extent that any future Inspectiv Services feature involves such automated decision-making with respect to Personal Data, Inspectiv will notify Customer in advance and the Parties will cooperate to ensure appropriate safeguards are in place as required by applicable Data Protection Laws, including providing data subjects with any rights of review, explanation or objection required by law.

14. Governing Laws This DPA will be governed by and construed in accordance with the Laws of the State of California, without prejudice to the provisions of the Laws of the country where the Customer has its principal place of business that cannot be derogated from contractually and without regard to conflict of law principles (as such Laws are applied to agreements entered into and to be performed entirely within California between residents of California).

15. Change in Laws If any variation is required to this DPA as a result of a change in or subsequently applicable Data Protection Laws or if the SCCs, as clarified, fail as a lawful data transfer mechanism, then either Party may provide written notice to the other Party of that change in laws. The Parties then will discuss and negotiate in good faith any variations to this DPA necessary to address such changes, with a view to agreeing and implementing those or alternative variations as soon as practicable.

Data Processing Addendum - Schedule 1

Inspectiv Sub-processors

Sub-processor	Nature and Purpose of Processing	Data Privacy Compliance Policy	Location of Processing	EU & UK Data Transfer Mechanism
Addapptation Inc. d/b/a Propensity	Account-based marketing	https://www.propensity.com/propensity-privacy-policy	United States	
Amazon Web Services, Inc.	Cloud data hosting	https://aws.amazon.com/compliance/data-privacy-faq/	United States	SCC
Atlassian, Inc.	Customer Support	https://www.atlassian.com/legal/data-processing-addendum#description-of-processing	United States	SCC
HubSpot Inc.	Marketing automation	https://legal.hubspot.com/dpa	United States	SCC
Nooks Communications, Inc.	Sales engagement and outbound communications, including SMS/text messaging	https://www.nooks.ai/dpa	United States	SCC
PostHog, Inc.	Product Analytics	https://posthog.com/docs/privacy/gdpr-compliance	United States	SCC
Salesforce.com Inc.	Customer service case management, authentication, chat and email communications	https://www.salesforce.com/form/other/privacy-request/	United States	SCC
ZoomInfo	Chorus (call recordings)	https://www.zoominfo.com/legal/privacy-policy?	United States	SCC