DATA PROCESSING ADDENDUM

Last Updated: September 10, 2021

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement or other written or electronic agreements between Insider and Customer (the "**Agreement**") for the purchase of online services from Insider (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Insider processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Insider may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules.

DATA PROCESSING TERMS

1. DEFINITIONS

"Authorized Affiliate" means any of Customer's Affiliate(s) which (i) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states and/or the United Kingdom, and (ii) is permitted to use the Services pursuant to the Agreement between Customer and Insider but has not signed its own Order Form with Insider and is not a "Customer" as defined under the Agreement.

"CCPA" means the California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, as the same may be amended from time to time.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means what is defined in the Agreement as "Customer Data."

"Data Protection Laws and Regulations" means all laws and regulations, including GDPR and CCPA, applicable to a Party in its use or provision of the Services, in connection with the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

"Data Subject Right" means any right afforded to a Data Subject under Data Protection Laws and Regulations, including the rights to access, rectify, restrict the Processing of Personal Data, erasure (including the right to be forgotten), data portability, objecting to the Processing, or to not be subject to an automated individual decision making.

"GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable natural person where such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Personal Data Breach" means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Insider or its Sub-processors of which Insider becomes aware.

"Security, Privacy and Architecture Datasheet" means the Security, Privacy and Architecture Datasheet for the Insider Services, as updated from time to time.

"Standard Contractual Clauses" or **"SCC"** means the agreement by and between Customer and Insider, pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, a copy of which can be found at https://www.useinsider.com/legal.

"Sub-processor" means any Processor engaged by Insider or its Affiliates engaged in the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1 Details of the Processing. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Insider is the Processor and that Insider or its Affiliates engaged in the Processing of Personal Data will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below. The subject- matter of Processing of Personal Data by Insider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 3 (Details of the Processing) to this DPA.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. This DPA and the Agreement are, at the time of signature of the Agreement, Customer's complete and final documented instructions to Insider for the Processing of Personal Data, and Customer's configuration of the Services shall constitute an additional instruction to Insider. Any additional or alternate instructions must be agreed upon separately. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data.

2.3 Insider's Processing of Personal Data. Insider shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of Customer and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Insider will Process Personal Data in compliance with applicable Data Protection Laws and Regulations, provided however that Insider shall not be in violation of this contractual obligation in the event that Insider's Processing of Personal Data in non-compliance with applicable Data Protection Laws and Regulations is due to Customer.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Requests. Insider shall, to the extent legally permitted and to the extent Insider has been able to identify that the request comes from a Data Subject whose Personal Data was submitted to the Services by Customer, promptly notify Customer if Insider receives a request from a Data Subject in relation to the exercise of any Data Subject Right ("**Data Subject Request**"). Insider will confirm to the Data Subject that it has passed the request to the Customer, but Insider shall not handle or execute the Data Subject Request.

3.2 Taking into account the nature of the Processing, Insider shall assist Customer by providing appropriate and necessary technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

4. INSIDER PERSONNEL

4.1 Confidentiality. Insider shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Insider shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Insider shall take commercially reasonable steps to ensure the reliability of any Insider personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Insider shall ensure that Insider's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Data Protection Officer. Insider has appointed a data protection officer for Insider and its Affiliates. The appointed person can be reached at privacy@useinsider.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Insider's Affiliates may be retained as Sub-processors; and (b) Insider and Insider's Affiliates respectively may engage third-party Sub-processors in connection with the

provision of the Services. Insider or a Insider' Affiliates has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the product or/and services provided by such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Attached hereto as Schedule 2 is a current list of Sub-processors for the Services. Such Sub-processors list shall include the identities of those Sub-processors, their country of location as well as the type of processing they perform. Insider will notify Customer of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3 Objection Right for New Sub-processors. Customer may object to Insider's use of a new Sub-processor by notifying Insider promptly in writing within ten (10) business days after receipt of Insider's notice in accordance with Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Insider will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Insider is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Insider without the use of the objected-to new Sub-processor, by providing written notice to Insider. Insider will refund to Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4 Liability for Sub-processors. Insider shall be liable for the acts and omissions of its Sub-processors to the same extent Insider would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1 Controls for the Protection of Customer Data. Insider shall maintain appropriate technical and organizational measures for protection of the security (including protection against Personal Data Breach), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Datasheet attached hereto as Schedule 1. Insider regularly monitors compliance with these measures. Customer is responsible for reviewing the information made available by Insider relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws and Regulations. Customer acknowledges that the security measures described within the Security, Privacy and Architecture Datasheet are subject to technical progress and development and that Insider may update or modify such document from time to time provided that such updates and modifications do not result in a material decrease of the overall security of the Services during a subscription term.

6.2 Customer Data Incident Management and Notification. Insider maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Datasheet and shall notify Customer without undue delay after becoming aware of a Personal Data Breach. Insider shall provide information to Customer necessary to enable Customer to comply with its obligations under Data Protection Laws and Regulations in relation to such Personal Data Breach. The content of such communication to Customer will (i) include the nature of Processing and the information available to Insider, and (ii) take into account that under applicable Data Protection Laws and Regulations, Customer may need to notify regulators or individuals of the following: (a) a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of Personal Data records concerned; (b) a description of the likely consequences of the Personal Data Breach; and (c) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Insider shall make commercially reasonable efforts to identify the cause of such Personal Data Breach and take those steps as Insider deems necessary and reasonable in order to remediate the cause of such Personal Data Breach to the extent the remediation is within Insider's reasonable control. The obligation to remediate the cause of a Personal Data Breach shall not apply to Personal Data Breaches that are caused by Customer or Customer's Users.

6.3 Third-Party Certifications and Audits. Insider has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Datasheet. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Insider shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of Insider and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement) a copy of Insider's then most recent third-party audits or certifications, as applicable, that Insider makes available to its customers

generally.

7. RETURN AND DELETION OF CUSTOMER DATA

Insider shall return Customer Data by enabling Customer to export its Customer Data as set forth in the Agreement and shall delete Customer Data, in accordance with this DPA, the Agreement, applicable laws and the Documentation.

8. AFFILIATES

8.1 Relationship between Insider and Customer's Authorized Affiliates. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing an independent DPA between Insider and each such Authorized Affiliate, subject to the provisions of the Agreement and this Section 8 and Section 9. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For sake of clarity, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

8.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Insider under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates and Authorized Affiliates.

8.3 Data Controller Rights of Affiliates and Authorized Affiliates. Any Affiliate or Authorized Affiliate shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

Except where applicable Data Protection Laws and Regulations require the Affiliate or Authorized Affiliate to exercise a right or seek any remedy under this DPA against Insider directly by itself, the parties agree that:

(i) solely the Customer that is the contracting party to the Agreement shall exercise any such right (including any Audit right) or seek any such remedy on behalf of such Affiliate or Authorized Affiliate,

(ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Affiliate or Authorized Affiliate individually but in a combined manner for all of its Affiliate and Authorized Affiliates together, and

(iii) when carrying out an on-site Audit, take all reasonable measures to limit any impact on Insider and its Sub- Processors by combining, to the extent reasonably possible, several Audit requests carried out on behalf of different Affiliate and Authorized Affiliates in one single Audit.

For the purpose of this Section 8.3, an Affiliate signing an Order Form with Insider is not deemed "Customer".

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Insider, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

10. EUROPEAN SPECIFIC PROVISIONS

10.1 Data Protection Impact Assessment. Upon Customer's request, Insider shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Insider. Insider shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined in the GDPR) in the performance of its tasks relating to this Section 10.1 of this DPA, to the extent required under the GDPR.

10.2 Infringing instructions. Insider shall immediately inform the Customer if, in its opinion, an instruction infringes GDPR.

10.3 European audit right. Where Customer or an Affiliate or an Authorized Affiliate is subject to the privacy laws of the European Union, Switzerland, the European Economic Area and/or their member states and the United Kingdom, Insider shall allow for and contribute to audits and inspections ("Audits") conducted by Customer (or Customer's independent, third-party auditor that is not a

competitor of Insider and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement), by providing any information regarding Insider's compliance with the obligations set forth in this DPA in the form of a copy of Insider's then most recent third-party audits or certifications, as applicable, that Insider makes available to its customers generally. Where Customer wishes to perform an on-site Audit, Customer may do so up to one (1) time per year, with at least three (3) week's advance written notice, unless otherwise required by Customer's, or its Affiliate's or Authorized Affiliate's regulators or law applicable to either of them. If Customer requests an on-site Audit, the following terms shall apply: (a) such Audit shall be limited to facilities operated by Insider, (b) such Audit shall not exceed one (1) business day; (c) before the commencement of any such Audit, Customer and Insider shall mutually agree upon the scope, cost and timing of the Audit; and (d) Customer shall promptly notify Insider with information regarding any non-compliance discovered during the course of an Audit.

10.4 Transfer mechanism(s) for data transfers. As of the Effective Date of this DPA, with regard to any transfers of Personal Data under this DPA from the European Union, Switzerland, the European Economic Area and/or their member states and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, Insider makes available the following transfer mechanism(s) which shall apply, in the order of precedence as set out below, if applicable:

i. Any valid transfer mechanism pursuant to Chapter V "Transfers of personal data to third countries or international organisations" of the GDPR permitting transfer of EU Personal Data outside the EU to which Insider would subscribe, certify or participate in.

ii. The Standard Contractual Clauses, in accordance with the following terms:

1. For purposes of the SCC, when and as applicable, Customer and any applicable Authorized Affiliates are each the data exporter, and Customer's signing of this DPA or an Agreement referencing this DPA, or a Customer's Affiliate signing an Order Form under an Agreement referencing this DPA, shall be treated as signing of the SCC and their appendices. Insider's signature of this DPA or an Agreement referencing this DPA shall be treated as signing of the SCC and their appendices. Details required under the SCC's Appendix 1 are available in Schedule 3 to this DPA and under the SCC's Appendix 2 are outlined in Schedule 1 to this DPA. In the event of any conflict or inconsistency between this DPA and the SCC, the SCC shall prevail.

2. Section 5 of this DPA represents Customer's express consent regarding existing and new Sub-processors under Clause 5(h) of the SCC. Copies of the Sub-processor agreements that must be provided by Insider to Customer pursuant to Clause 5(j) of the SCC may have all commercial information, or clauses unrelated to the SCC or their equivalent, removed by Insider beforehand; such copies will only be provided by Insider upon request by Customer.

3. Audits pursuant to Clause 5(f) and Clause 12(2) of the SCC shall be carried out in accordance with Section 10.3 above.

4. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the SCC shall only be provided by Insider to Customer upon Customer's request.

11. CALIFORNIA CONSUMER PRIVACY ACT OF 2018

11.1 The following shall apply for Customers subject to the CCPA:

a) All references to Data Protection Laws and Regulations in this DPA shall be deemed to include a reference to the CCPA;

b) All references to Personal Data in this DPA shall be deemed to include Personal Information, as defined in the CCPA, provided such data is Customer Data;

c) All references to "Controller" in this DPA shall be deemed to be references to "**Business**," as defined in the CCPA;

d) All references to "Processor" in this DPA shall be deemed to be references to "**Service Provider**," as defined in the CCPA;

e) Any capitalized term used in this Section 11 but not defined herein, shall have the meaning set forth in the CCPA.

11.2 Insider shall not Sell any Personal Information.

11.3 Insider will Process Personal Information solely as set forth in Section 2.3 (the "**Business Purpose**"), and shall not retain, use, or disclose the Personal Information for any purpose other than the Business Purpose.

11.4 Insider does not receive any Personal Information from Customer as consideration for Insider's provision of the Services.

11.5 Insider certifies that it understands the restrictions set forth in this Section 11 and will comply with them.

List of Schedules:

Schedule 1: Insider Security, Privacy and Architecture Datasheet

Schedule 2: List of Sub-Processors as of the Effective Date

Schedule 3: Details of the Processing

SCHEDULE 1

Insider Security, Privacy, and Architecture Information Security Datasheet

Introduction

The goal of this document is to provide high-level information to our customers regarding Insider's commitment to security and data protection.

Insider's Corporate Trust Commitment

Insider is committed to achieving and maintaining the trust of our customers. Our goal is to be as transparent as possible with our customers in offering state-of-the-art security and protections to meet and exceed expectations in today's modern computing world.

Policy Ownership

Insider has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of the Insider Security Team.

Insider Infrastructure

Insider hosts the Insider Services with Amazon Web Services in their EU-West-1 region, Ireland.

Third-Party Architecture

Insider may use one or more third-party content delivery networks to provide the Insider Services and to optimize content delivery via the Insider Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the Insider Services, may be cached with such content delivery networks to expedite transmission. Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

Audits, Certifications, and Regulatory Compliance

Insider is ISO/IEC 27001 certified and has the SOC 2 Type 1 report. Insider also enters into the EU Standard Contractual Clauses with its Customers who would like to be protected with applicable data transfer mechanism under the GDPR.

Security Controls

1. Organization Security

Insider's CTO is responsible for the overall security of the Insider Services, including oversight and accountability. Insider's contracts with third-party hosting providers such as Amazon Web Services include industry-standard information protection requirements.

2. Asset Classification and Logical Access Control

Insider maintains an inventory of essential information assets such as servers, databases, and information. All Customer Data is classified as Confidential by Insider.

Insider adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. Insider maintains separate development, staging (or sandbox), user acceptance testing, and production environments access to each environment and within each environment is strictly controlled.

Access to Insider's servers are controlled via revocable SSH keys managed via configuration management and rotated at least annually. All access to Insider's servers or Customer Data is logged and can only be accessed through Insider's VPN, which uses multi-factor authentication. Database access is controlled via 24-character passwords with IP whitelisting. Insider's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.

3. Personnel Security

All employees at Insider sign a non-disclosure agreement when their employment begins. In addition, Insider conducts background checks of its employees as part of its onboarding process. All employees are informed of, and agree to comply with, Insider's security policies and practices as a part of their initial onboarding.

System administrators, developers and other users with privileged access receive special and ongoing training and are subjected to additional background screening.

4. Physical and Environmental Security

Access to Insider facilities is controlled by 24-hour security. Additionally, all Insider offices are protected by locked access and are under 24-hour video surveillance. All Insider employee workstations are encrypted and password protected, and all Insider user accounts require two-factor authentication.

Data centers and servers are managed and controlled by our Cloud hosting providers. Insider employees have no access to any of these data centers.

Details regarding the security practices & controls applicable to these facilities can be found at their websites: AWS:

https://aws.amazon.com/security

5. Policies and Logging

The Insider Services are operated in accordance with the following procedures to enhance security:

- User passwords are never transmitted or stored in clear text
- Insider uses industry-standard methods to determine password validity
- Insider keeps audit logs for all access to production servers
- Server access is controlled via Amazon Web Services Identity and Access Management
- Logs are stored in a secure centralized host to prevent tampering
- Passwords are not logged under any circumstances
- All access to customer dashboard accounts by Insider Employees must be done through an internal service that is accessible via a 2-factor VPN only
- As part of Insider's Employee Information Security Policy, employees may not store any Customer Data on removable media

6. Intrusion Detection

Insider monitors system, user, and file behavior across its infrastructure using a host-based Intrusion Detection System. Intrusion Detection alerts are monitored by the Security and DevOps teams 24/7. Additionally, Insider may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Insider Services function properly.

Insider's APIs and Dashboard use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and automatically alert Insider's engineering team.

7. Security Logs

All Insider systems used in the provision of the Insider Services, including firewalls, routers, network switches, and operating systems log information to their respective system log facility in order to enable security reviews and analysis.

8. System Patching and Configuration Management

Insider patches its servers and rebuilds its entire cloud infrastructure from configuration management systems on a regular basis, which ensures that the latest patches are applied and that we "reset" back to a known, clean state. Insider maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

9. Vulnerability Management

Insider's infrastructure and applications are continuously scanned by a Vulnerability Management System. Alerts are monitored by our Security Team and addressed at least monthly by the Insider Security Team. Insider also maintains a list membership to various CVE vulnerability mailing lists. Patches and 'critical' and 'high' vulnerabilities are remediated no later than 30 days following discovery.

Insider also uses static code analysis tools during the build process (such as Brakeman and bundler-audit) to perform static security analysis.

10. Third-Party Penetration Testing

Insider undergoes a third-party penetration test of the Insider Services on an annual basis.

11. Monitoring

For technical monitoring, maintenance and support processes, Insider uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- APM performance monitoring
- Latency monitoring
- Error monitoring

12. Customer Access Control

The Insider Services employ a variety of security controls. These include, but are not limited to:

● API IP Whitelisting - Defines the range of IP addresses from which a customer's users can access the Insider API to prevent unauthorized third parties from accessing the Insider Services.
● All requests on the Insider Dashboard have cross-site request forgery (CSRF) protection. All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
● Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.

13. Development and Maintenance

Insider uses tools such as GitHub to effectively manage the development lifecycle. During testing, Insider generates test accounts and fake data for testing. Insider does not use production data in test accounts.

Application source control is accomplished through private GitHub repositories. Insider has controls in place to ensure that all code must be approved before being merged to Insider's main code branch; only authorized employees are granted access to promote code to production.

Insider developers receive additional security training as part of their onboarding, and undergo regular and periodic security training during the term of their employment. Insider maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

14. Malware Prevention

Insider adopts the principle of least privilege for all accounts running application or database services. Proper change management ensures that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Insider employee computers have virus scanners installed and updated definitions sent out from a central device management platform.

15. Information Security Incident Management

Insider maintains written and regularly-audited security incident management policies and procedures, including an Incident Response Plan to be enacted in the event of an incident.

16. Data Encryption

The Insider Services use industry-accepted encryption practices to protect Customer Data and communications during transmissions between a customer's network and the Insider Services, including 256-bit TLS Certificates and 4096-bit RSA public keys at a minimum.

Insider audits the TLS ciphers used in connection with the provision of the Services with third-party security auditors to ensure that anonymous or weak ciphers are not used. These audits also confirm that the Services do not allow client renegotiation, support downgrade attack protection and forward secrecy.

Data shipped to Amazon Web Services is encrypted in transit and at-rest using AES-256 encryption via Amazon's managed encryption key process.

Where use of the Services requires a customer to provide access to third party services, Insider performs additional encryption of that information.

17. Return and Deletion of Customer Data

The Insider Services allow import, export, and deletion of Customer Data by authorized users at all times during the term of a customer's subscription. Following termination or expiration of the Services, Insider shall securely overwrite or delete Customer Data within 180 days following any such termination, in accordance with the Agreement, applicable laws and the Documentation.

18. Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Insider Services is stored on a multiple database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

19. Business Continuity Management and Disaster Recovery

Insider has a formal and documented Business Continuity Procedure and Disaster Recovery Plan, which is tested annually. Insider tests database backups and failovers as part of our Business Continuity Plan.

20. Blocking Third Party Access

The Insider Services have not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access Customer Data. We do not voluntarily provide any government or other third party with encryption keys, or any

other way to break our encryption.

21. Contacts

Insider's Security Team can be reached by emailing security@useinsider.com.

SCHEDULE 2

SUB-PROCESSORS USED IN CONNECTION WITH THE INSIDER SERVICES

This Schedule describes the Sub-processors material to Insider's provision of the Insider Services.

Insider ("Insider") uses certain Sub-processors, including certain subsidiaries of Insider (as described below) in connection with its provision of the Insider Services to its customers. What follows is the full list of Sub-processors that Insider uses in its provision of the Insider Services. Depending upon a Customer's use of the Insider Services e.g. geographical location of the Customer, not all Sub-Processors will be needed to deliver the Insider Services.

As used herein, Sub-processors refer to Affiliates of Insider and third parties who process Personal Data on behalf of Insider. Third parties engaged by Insider as Sub-processors are subject to written agreements that contain confidentiality and security commitments not less protective than those in the DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. Insider remains responsible for the acts and omissions of its Sub- processors pursuant to the DPA. Terms used herein without definition are used as defined in the MSA.

Infrastructure Sub-processors – Storage of Personal Data

Entity Name	Services Provided	Location of Processing
Amazon Web Services Ireland Ltd.	Third-party hosting provider.	European Union

Sub-processors – Other Personal Data Processing as set forth below

Entity Name	Services Provided	Location of Processing
SendGrid, Inc.	Email delivery provider.	United States
AMD Telecom	SMS delivery provider.	European Union
Countly Ltd.	Product Plug-in	European Union
Google RBM	Message delivery provider.	United States
Zendesk, Inc.	Message delivery provider.	United States

Content Delivery Networks

The Insider Services use content delivery networks ("CDNs") to provide the Insider Services, for security purposes, to support user authentication, and to optimize content delivery. CDNs are commonly used systems of distributed services that deliver content based on the geographic location of the individual accessing the content and the origin of the content provider. Content items that are transmitted via CDNs tend to be high content data (videos, images) that have been uploaded to the Insider Services and may be cached by a CDN to expedite delivery of such content to End Users.

Name of CDN	Description of CDN Services	Location of Processing
Amazon Web Services, Inc.	Content delivery network used by Insider to optimize content delivery.	Global
Cloudflare, Inc.	Content delivery network used by Insider to optimize content delivery.	Global

SCHEDULE 3

DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Insider will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 7 of the DPA, Insider will Process Personal Data for the Term of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which include Personal Data relating to the End Users.

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which include the following categories of Personal Data:

Customer transaction information (order/request information)

Marketing information (information obtained through Insider Java Script which is cookie-similar tech)

Click information

Duration of stay on the site/advertisement

IP address

Although it is not included in the ordinary course of Insider Services, if Customer prefer to send the following data to use specific features of the Insider Services, Insider will process the following categories of Personal Data:

Contact Information (Email)

Identity information (Name, surname, age, gender)