DATA PROCESSING ADDENDUM

Note to copy:
The Insider Data Processing Addendum is made available at https://useinsider.com/legal/dpa/.
For Customers that would like to receive a signed copy of the Insider Data Processing Addendum, we have made this copy available to you. This copy includes signatures on the Data Processing Addendum version last modified June 10, 2024 . Insider and its affiliates do not accept any changes to be made in this copy unless agreed by the Parties and made in writing.
Please note that we update the Data Processing Agreement as we describe in the 'Amendments' article below. Current Data Processing Agreement terms are available at "https://useinsider.com/legal/dpa/" .
If you have any questions, please contact your Insider representative

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/or any other data protection laws and regulation from other countries in which Customer or their Authorized Affiliate are based or provides services, including but not limited the Republic of Brazil, 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.
"Insider Affiliate" means any companies in which the Insider is a shareholder and/or has a say in its management.
"CPRA" means the California Privacy Rights Act 2020, 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" shall mean all electronic data or information submitted by or on behalf of Customer to, or collected from the Customer Application by the Insider Services.
"Data Protection Laws and Regulations" means all laws and regulations, including GDPR, and CPRA, 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.
"Documentation" means any printed or digital document, Insider Academy content, presentation, information or document shared in relation to Insider products and services and Insider's data processing activities.
"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 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 Schedule 2 "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. Customer is responsible for all actions taken by Customer or its Users in the Customer's Account(s) and for Users' compliance with this Agreement. Customer shall provide adequate notice and obtain valid consent for the use of tracking technologies used by the Insider Services in creating End User profiles which, if Customer is established in the EEA or if Customer uses the Insider Services in relation to EEA residents, must comply with arts. 13 and 7 GDPR. 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 Customer's Users in their use of the Services; (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 and (iv) Processing when it sells services based on the given intellectual property right; on the grounds of data transfers to be made in order to provide the service to the main owner of the right . 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 Schedule 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, Insider and Insider's Affiliates, 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 organizations" 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. In the event of any conflict or inconsistency between this DPA and the SCC, the SCC shall prevail.

2. Schedule 2 of this DPA represents Customer's express consent regarding existing and new Sub-processors.

11.AMENDMENTS

Notwithstanding anything else to the contrary in the Agreement we reserve the right to make any updates and changes to this DPA and the terms that apply in the 'Amendment; No Waiver' section of the Master Terms will apply.

12. SEVERABILITY

If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

13. California Privacy Rights Act of 2020

13.1 The following shall apply for Customers subject to the CPRA:

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

b) All references to Personal Data in this DPA shall be deemed to include Personal Information, as defined in the CPRA, 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 CPRA;

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

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

13.2 Insider shall not Sell any Personal Information.

13.3 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.

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

13.5 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 mechanisms 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 and for its own products 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

The list of sub-processors of Insider is available at https://useinsider.com/legal/subprocessors

SCHEDULE 3
DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Insider will Process Personal Data as necessary to perpform 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 (customers of the Customer).

Type of Personal Data

Transaction information (order /request information of end-user of the Customer)
Marketing information (information obtained through Insider Java Script which is cookie-similar tech)
Click information
Browsing Behavior (Pages visited on the website, Products or services viewed, Time spent on each page, Frequency of visits)
Duration of stay on the site/advertisement
IP address
Survey Responses
Purchase History (Items purchased, Transaction history, Order Value)
Device Information (Device type (desktop, mobile, tablet), Operating system, Browser type and version)

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, Phone Number)
Identity information (Name, Surname, Age, Gender, Birthday of Website Users, Location, IDFA)

ACCEPTED BY CUSTOMER	**ACCEPTED BY INSIDER**
SIGNATURE:_____	**SIGNATURE:**_____
FULL NAME:_____	**FULL NAME:**_____
TITLE:_____	**TITLE:**_____
DATE:_____	**DATE:**_____

Annex 1: STANDARD CONTRACTUAL CLAUSES

The purpose of these standard contractual clauses to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer).The standard contractual clauses also set out the rights and obligations of controllers and processors with respect to the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679, as regards the transfer of personal data from a controller to a processor, or from a processor to a sub-processor.

Each "**Party"**; together "**Parties**", have agreed on the following Contractual Clauses ("**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.

These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1), and Article 46 (2)(c) of GDPR and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of GDPR, provided they are not modified, except to add or update information in the Annexes. This does not prevent the Parties from including the standard contractual clauses laid down in this Clauses in a wider contract, and to add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the GDPR.

These Clauses apply with respect to the transfer of personal data as specified in Clause 2.

Clause 1
Definitions

1.1. The terms defined below shall have the same meaning as in GDPR; the terms, therefore shall be read and interpreted in the light of the provisions of GDPR
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 sub-processor' means any processor engaged by the Data Importer or by any other Sub-processor of the Data Importer who agrees to receive from the Data Importer or from any other sub-processor of the Data Importer Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
1.2 These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in GDPR.

Clause 2

Details of the transfer
The details of the transfer and in particular the special categories of Personal Data that are transferred and the purposes for which they are transferred, are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause
3.1 Data subjects may invoke and enforce these Clauses, as third party beneficiaries, against the data exporter and / or data importer, with the following exceptions:
(i) Clauses regarding purpose and scope,third party beneficiaries, definition, hierarchy, and description of transfer
(ii) Clause on documentation compliance
(iii) Clause on notification
(iv) Clause regarding use of sub-processor
(v) Clause regarding liability;
(vi) Indemnification clause;
(vii) Supervision clause;
(viii) Non-compliance and jurisdiction clauses i.

Clause 4
Obligations of the Data Exporter
The data exporter warrants that it has used reasonable efforts to determine that the data
importer is able to satisfy its obligations under this Clause as a safeguard:
4.1. 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;
4.2. 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 and the Data Importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 1.
4.3. that the Data Importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
4.4. 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, unauthorized 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;
4.5. that it will ensure compliance with the security measures;
4.6. 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 GDPR;
4.7. to forward any notification received from the Data Importer or any sub-processor 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;
4.8. 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 sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
4.9. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the Data Importer under the Clauses; and
4.10. that it will ensure compliance with Clause 4(a) to (i)

4.11. not only Data Exporter but also Data Importer shall provide the data subject with a copy of the Clauses upon request. To the extent necessary to protect business secrets or other confidential information, including the measures described in Appendix 1I, the Parties may redact the text of the Appendixes to these Clauses prior to sharing a copy, but shall provide a meaningful summary where otherwise the data subject would not be able to understand the content of the Appendixes. This is notwithstanding the obligations of the data exporter under Articles 13 and 14 of GDPR, in particular to inform the data subject about the transfer of special categories of.

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

5.1. 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;

5.2. to process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 1.

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

5.4. that the processing by the data importer shall only take place for the duration specified in Appendix 1. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to the requirement for the data importer to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of the GDPR.

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

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

5.7. that where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Appendix 2.

5.8. that the data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.
5.9. that the data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
5.10. 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;
5.11. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the Personal Data transferred;
5.12. 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 unauthorized access, and
*iii.*any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
5.13. that the data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Appendix 1I the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
5.14. 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;
5.15. 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;
5.16. that data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
5.17. that the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
5.18. to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of 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;
5.19. that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;
5.20. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
5.21. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the Data Exporter.
5.22. To cooperate in good faith with and assist the Data Exporter in any way necessary to enable the data exporter to comply with its obligations under the GDPR, notably to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the Data Importer.

Clause 6
Liability
6.1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the Data Exporter for the damage suffered.
6.2. Each Party shall be liable to the other Party/ies for any material or non-material damages it causes the other Party/ies by any breach of these Clauses. Liability as between the Parties is limited to actual damage suffered. Punitive damages are excluded.
6.3. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party

beneficiary rights under these Clauses.

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

6.5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties. The Parties agree that if one Party is held liable, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

6.7. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or its sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the data subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract of by operation of law, in which case the Data Subject can enforce its rights against such entity.

6.8. The Data Importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities and may not invoke the conduct of a sub-processor

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

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

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

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

(ii) refer the dispute to the competent courts.

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

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

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

Clause 7

Mediation and jurisdiction

7.1. 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:

i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

ii. to refer the dispute to the courts in the Member State in which the Data Exporter is established.

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

8.1. 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.
8.2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.
8.3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the Data Importer, or any sub-processor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law and Choice of Forum
9.1. The Clauses shall be governed by the law of the Member State in which the Data Exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.
9.2. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
9.3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
9.4. The Parties agree to submit themselves to the jurisdiction of such courts.

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
11.1. 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. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the Data Importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the sub-processor's obligations under such agreement.
11.2. The prior written contract between the Data Importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or the Data Importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
11.3. The provisions relating to data protection aspects for sub-processing 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.
11.4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.
11.5. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and subsequent amendments.
11.6. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its

obligations under that contract.

11.7. The data importer shall agree a third party beneficiary clause with the sub-processor whereby, in the event of bankruptcy of the data importer, the data exporter shall be a third party beneficiary to the sub-processor contract and shall have the right to enforce the contract against the sub-processor, including where applicable by instructing the sub-processor to erase or return the personal data.

Clause 12

Obligation after the termination of personal data processing services

12.1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the sub-processor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

Clause 13

Hierarchy

In the event of a conflict between these Clauses and the provisions of any other agreement between the Parties existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 14

Local laws affecting compliance with the Clauses

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

14.2. The Parties declare that in providing the warranty in Article 14.1, they have taken due account in particular of the following elements: (i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred; (ii) the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorizing access by such authorities, as well as the applicable limitations and safeguards; (iii) any safeguards in addition to those under these Clauses, including the technical and organizational measures applied during transmission and to the processing of the personal data in the country of destination.

14.3. The data importer warrants that, in carrying out the assessment under Article 14.2, it has made best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses

Clause 15

Obligations of the data importer in case of government access requests

***15.1** Notification*

15.1.1. The data importer agrees to promptly notify the data exporter and, where possible, the data subject (if necessary with the help of the data exporter) if it: (i) receives a legally binding request by a public authority under the laws of the country of destination for disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; EN 15 EN (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

15.1.2. If the data importer is prohibited from notifying the data exporter and / or the data subject, the data importer agrees to use its

best efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them upon request of the data exporter.

15.1.3. To the extent permissible under the laws of the country of destination, the data importer agrees to provide to the data exporter, in regular intervals for the duration of the contract, the greatest possible amount of relevant information on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.).

15.1.4. The data importer agrees to preserve the information pursuant to Article 15.1.1 to 15.1.3 for the duration of the contract and make it available to the competent supervisory authority upon request.

15.1.5. Article 15.1.1 to 15.1.3 are notwithstanding the obligation of the data importer pursuant to termination clause to promptly inform the data exporter where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

15.2.1. The data importer agrees to review, under the laws of the country of destination, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the data importer pursuant to Article 15.1.5.

15.2.2. The data importer agrees to document its legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make it available to the data exporter. It shall also make it available to the competent supervisory authority upon request.

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

Clause 16

Non-compliance with the Clauses and termination

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

16.2. 16.2 In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated.

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

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

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

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

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

16.4. Personal data that has been transferred prior to the termination of the contract pursuant to Article 16.3 shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17
Docking clause
17.1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
17.2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
17.3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

On behalf of the Data Exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

On behalf of the Data Importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

Appendix 1

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's business or organization type is (please specify briefly your activities relevant to the transfer):

☐Central government
☐ Charitable and voluntary
☐ Education and childcare
☐ Finance, insurance and credit
☐ General business
☐ Health
☐ IT, digital, technology and telecoms
☐ Justice and policing
☐ Land and property services
☐ Legal and professional advisers
☐ Local government
☐ Marketing and research
☐ Media
☐ Membership association
☐ Political
☐ Regulators
☐ Religious
☐ Research
☐ Retail and manufacture
☐ Social care
☐ Trade, employer associations, and professional bodies
☐ Traders in personal data
☐ Transport and leisure
☐ Utilities and natural resources
☐ Other – Please add details:

The data exporter is using the personal data which is being transferred for the following purposes or activities:

☐ Standard business activities, which apply to most businesses and organizations
☐ Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter's staff.
☐ Advertising, marketing and public relations of the data exporter's own business or activity, goods or services.
☐ Accounts and records, including

- keeping accounts relating to the data exporter's business or activity;
- deciding whether to accept any person or organization as a customer;
- keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;
- keeping customer records
- records for making financial or management forecasts; and
- other general record keeping and information management.

Other activities:

☐ Accounting and auditing services
☐ Administration of justice, including internal administration and management of courts of law, or tribunals and discharge of court business.
☐ Administration of membership or supporter records.
☐ Advertising, marketing and public relations for others, including public relations work, advertising and marketing, host mailings for other organizations, and list broking.
☐ Assessment and collection of taxes, duties, levies and other revenue
☐ Benefits, welfare, grants and loans administration
☐ Canvassing, seeking and maintaining political support amongst the electorate.
☐ Constituency casework on behalf of individual constituents by elected representatives.
☐ Consultancy and advisory services, including giving advice or rendering professional services, and the provision of services of an advisory, consultancy or intermediary nature.
☐ Credit referencing, including the provision of information by credit reference agencies relating to the financial status of individuals or organizations on behalf of other organizations
☐ Data analytics, including profiling
☐ Debt administration and factoring, including the tracing of consumer and commercial debtors and the collection on behalf of creditors, and the purchasing of consumer or trade debts from business, including rentals and installment credit payments.
☐ Education, including the provision of education or training as a primary function or as a business activity.
☐ Financial services and advice including the provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking
☐ Fundraising in support of the objectives of the data exporter
☐ Health administration and services, including the provision and administration of patient care.
☐ Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogs, lists, directories and bibliographic databases.
☐ Insurance administration including the administration of life, health, pensions, property, motor and other insurance business by an insurance firm, an insurance intermediary or consultant
☐ IT, digital, technology or telecom services, including use of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software
☐ Journalism and media, including the processing of journalistic, literary or artistic material made or intended to be made available to the public or any section of the public.
☐ Legal services, including advising and acting on behalf of clients.
☐ Licensing and registration, including the administration of licensing or maintenance of official registers.
☐ Not-for-profit organizations' activities, including
- establishing or maintaining membership of or support for a not-for-profit body or association, and
- providing or administering activities for individuals who are either members of the not-for-profit body or association or have regular contact with it.

☐ Pastoral care, including the administration of pastoral care by a vicar or other minister of religion.
☐ Pensions administration, including the administration of funded pensions or superannuation schemes.
☐ Procurement, including deciding whether to accept any person or organization as a supplier, and the administration of contracts, performance measures and other records.
☐ Private investigation, including the provision on a commercial basis of investigatory services according to instruction given by clients
☐ Property management, including the management and administration of land, property and residential property, and the estate management of other organizations.
☐ Realizing the objectives of a charitable organization or voluntary body, including the provision of goods and services in order to realize the objectives of the charity or voluntary body.
☐ Research in any field, including market, health, lifestyle, scientific or technical research.
☐ Security of people and property, including using CCTV systems for this purpose.
☐ Trading/sharing in personal information, including the sale, hire, exchange or disclosure of personal information to third parties in

return for goods/services/benefits.
☐ Other activities (please provide details):

Data Importer
The Data Importer is a Singapore based technology company which provides to the Data Exporter a growth management platform for its multichannel marketing activities.

Data Subjects
The Data Exporter may submit Personal Data to the Data Importer and its Affiliates, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:
-Prospective customers, customers, resellers, referrers, business partners, and vendors of the Data Exporter (who are natural persons);
-Employees or contact persons of the Data Exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);
-Employees, agents, advisors, and freelancers of the Data Exporter (who are natural persons); and/or
-Natural persons authorized by the Data Exporter to use the services provided by the Data Importer to the Data Exporter.

Categories of Data
The personal data transferred concern the following categories of data:

The Data Exporter may submit Personal Data to the Data Importer and its Affiliates, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:
☐ Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.
☐ Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organizations.
☐ Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records.
☐ Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records.
☐ Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information.
☐ Goods or services provided and related information, including details of the goods or services supplied, licenses issued, and contracts.
☐ Personal data relating to criminal convictions and offenses
☐ Other (please provide details of other data subjects):

Processing Operations
The personal data transferred will be subject to the following basic processing activities defined in this addendum.

☐ Receiving data, including collection, accessing, retrieval, recording, and data entry
☐ Holding data, including storage, organization and structuring
☐ Using data, including analyzing, consultation, testing, automated decision making and profiling
☐ Updating data, including correcting, adaptation, alteration, alignment and combination
☐ Protecting data, including restricting, encrypting, and security testing
☐ Returning data to the data exporter or data subject
☐ Erasing data, including destruction and deletion

Appendix 2

Security Measures

A. The Data Importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.
B. More specifically, the Data Importer/sub-processor's security program shall include:

Access of Data Importer's internal operations

The Data Importer/sub-processor implements optimal measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are processed or used, including:
- establishing security areas;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- The data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access of the system

The Data Importer implements optimal measures to prevent their data processing systems from being used by unauthorized persons, including:
- use of proper encryption technologies;
- identification of the terminal and/or the terminal user to the Data Importer/sub-processor and processing systems;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered and
- all access to data content is logged, monitored, and tracked.

Access to Use Specific Areas of Data Processing

The Data Importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:
- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and control of files, controlled and documented destruction of data.

Transportation

Data Importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:
- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and as far as possible, all data transmissions are logged, monitored and tracked.

Input

Data Importer/sub-processor implements suitable input control measures, including:
- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;

- utilization of unique authentication credentials or codes (passwords);
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within Data Importer/sub-processor's organization of the input authorization; and
- electronic recording of entries.

Documentation
Data Importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data Importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this DPA.

Control
Data Importer/sub-processor shall implement optimal measures to monitor access restrictions to Data Importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:
- individual appointment of system administrators;
- adoption of optimal measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the Data Importer/sub-processor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to the Data Exporter upon request.

On behalf of the Data Exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

On behalf of the Data Importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature: