DATA PROCESSING ADDENDUM

Exhibit C to the Master Subscription Agreement

Version 1.3

H&A Security Solutions, LLC d/b/a Tellaro — 12178 N 1450th Street, Effingham, Illinois 62401

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "DPA") forms part of the Master Subscription Agreement or, where applicable, the End User License Agreement — On-Prem (each, the "Agreement") between H&A Security Solutions, LLC d/b/a Tellaro ("Tellaro") and Customer and applies whenever Tellaro processes personal data on behalf of Customer in connection with the Service. Capitalized terms not defined here have the meanings given in the Agreement. In the event of conflict between this DPA and the Agreement, this DPA controls with respect to the processing of personal data.

1. DEFINITIONS

"Applicable Data Protection Laws" means all data protection and privacy laws applicable to a party's processing of personal data under the Agreement, including the California Consumer Privacy Act (as amended by the California Privacy Rights Act) ("CCPA"), other U.S. state privacy laws, and where applicable the EU and UK General Data Protection Regulations ("GDPR").

"Controller" means the natural or legal person which determines the purposes and means of the processing of personal data; for clarity, Customer is the Controller of Customer Personal Data.

"Customer Personal Data" means any personal data contained within Customer Data.

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

"Processor" means the natural or legal person which processes personal data on behalf of the Controller; for clarity, Tellaro is the Processor with respect to Customer Personal Data, except with respect to Threat Indicators and aggregated data used as permitted by Section 2.5.

"Sub-Processor" means a third party engaged by Tellaro to process Customer Personal Data, as listed in Schedule 1.

2. ROLES, SCOPE, AND INSTRUCTIONS

2.1 Role Allocation.

The parties acknowledge that, with respect to Customer Personal Data, Customer acts as Controller (or, where applicable, as a Processor on behalf of its own controllers), and Tellaro acts as Processor (or, where applicable, as a Sub-Processor).

2.2 Subject Matter and Duration.

The subject matter of the processing is Tellaro's provision of the Service to Customer. The duration of the processing is the term of the Agreement plus any post-termination data-export period set forth in the Agreement.

2.3 Categories of Data and Data Subjects.

The categories of personal data processed include identifiers, online identifiers, device identifiers, network and security telemetry, user activity data, and any personal data Customer chooses to submit. Categories of data subjects include Customer's employees, contractors, end users, and other persons whose data is captured in Customer security telemetry.

2.4 Documented Instructions.

Tellaro will process Customer Personal Data only on Customer's documented instructions, including those set out in the Agreement, this DPA, and Order Forms, or as required by law (in which case Tellaro will, where legally permitted, notify Customer before processing). Tellaro will not "sell" or "share" Customer Personal Data within the meaning of CCPA, will not retain, use, or disclose Customer Personal Data outside the direct business relationship between the parties, and will not combine Customer Personal Data with personal data received from other sources except as needed to provide the Service.

2.5 Threat Indicators and Aggregated Data.

Customer instructs Tellaro to use Threat Indicators and de-identified, aggregated data, each as described in the Agreement, to detect, prevent, and respond to security threats for Customer and Tellaro's other customers and to improve the Service. These uses are a permitted business purpose under the CCPA and part of Customer's documented instructions, and the restrictions in Section 2.4 do not prohibit them.

3. TELLARO OBLIGATIONS

3.1 Confidentiality.

Tellaro will ensure that personnel authorized to process Customer Personal Data are bound by appropriate confidentiality obligations.

3.2 Security.

Tellaro will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data, as further described in Schedule 2.

3.3 Assistance.

Tellaro will provide reasonable assistance to Customer (taking into account the nature of the processing and the information available) in: (a) responding to data-subject requests; (b) carrying out data protection impact assessments and consultations with supervisory authorities; and (c) fulfilling Customer's security and breach-notification obligations under Applicable Data Protection Laws. Assistance beyond what Tellaro provides to customers generally, or required because of Customer's own acts or omissions, is provided at Tellaro's then-current professional services rates.

3.4 Personal Data Breach Notification.

Tellaro will notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. Notice will include the information required under Applicable Data Protection Laws to the extent then known, and may be supplemented as information becomes available. Notice of a Personal Data Breach is not an acknowledgment of fault or liability. "Personal Data Breach" means a breach of Tellaro's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in Tellaro's possession or control.

3.5 Return or Deletion.

Upon expiration or termination of the Agreement, Tellaro will, at Customer's option, return or delete Customer Personal Data in accordance with the Agreement's post-termination data-export window. Tellaro may retain copies of Customer Personal Data as required by law, subject to continued protection under this DPA.

3.6 Records and Audits.

Tellaro will maintain records of its processing activities as required by Applicable Data Protection Laws and will make information reasonably necessary to demonstrate compliance with this DPA available to Customer. Tellaro's annual SOC 2 (or equivalent) report will satisfy this obligation in the ordinary course; additional audit rights are limited to once per year, on reasonable advance notice, during business hours, and at Customer's expense, conducted in a manner that does not interfere with Tellaro's operations or the security of other customers, by Customer or an independent auditor that is not a Tellaro competitor and is bound by confidentiality obligations acceptable to Tellaro.

4. SUB-PROCESSORS

4.1 General Authorization.

Customer authorizes Tellaro to engage the Sub-Processors listed in Schedule 1. Tellaro will impose data-protection obligations on each Sub-Processor that are no less protective than those in this DPA and remains responsible for each Sub-Processor's performance.

4.2 Changes.

Tellaro will notify Customer of new or replacement Sub-Processors at least thirty (30) days in advance (or, in the case of urgent security or operational needs, as soon as reasonably practicable). Customer may object on reasonable data-protection or security grounds within fifteen (15) days; if the parties cannot resolve the objection, Customer may terminate the affected Order Form for cause without penalty.

5. INTERNATIONAL TRANSFERS

Tellaro processes Customer Personal Data within the United States. Where Customer Personal Data is transferred from the European Economic Area (EEA), the United Kingdom, or Switzerland to the United States or to another country that has not been designated as providing an adequate level of protection, the parties agree that:

- the EU Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 (the "EU SCCs") are incorporated by reference, with Module Two (Controller-to-Processor) applying where Customer is a Controller and Module Three (Processor-to-Sub-Processor) applying where Customer is a Processor;
- the UK International Data Transfer Addendum to the EU SCCs (issued by the UK Information Commissioner) (the "UK Addendum") is incorporated by reference for transfers from the United Kingdom;
- for transfers from Switzerland, the EU SCCs apply with the modifications required by the Swiss Federal Data Protection Act and guidance from the Swiss Federal Data Protection and Information Commissioner;
- the populated Annexes I, II, and III to the EU SCCs are set forth in Schedule 3 of this DPA.

Customer acknowledges that Tellaro relies on the EU SCCs (and UK Addendum / Swiss equivalents, as applicable) as the lawful basis for international transfers. The parties

will cooperate in completing any transfer-impact assessment reasonably required by Applicable Data Protection Laws.

5.1 EU / UK Representative.

Tellaro will designate a representative in the EU and/or the UK pursuant to Article 27 of the GDPR (and the equivalent UK provision) if and when required by applicable law and Tellaro's processing activities. Where designated, the representative's contact details will be published at https://www.tellaro.io/legal.

6. TERM AND ORDER OF PRECEDENCE

This DPA is effective for the duration of the Agreement. In the event of conflict between this DPA and the Agreement, this DPA controls with respect to the processing of personal data.

Each party's liability arising out of or relating to this DPA (including, to the extent permitted by them, the Standard Contractual Clauses) is subject to the limitations and exclusions of liability in the Agreement, including the data protection super-cap.

SCHEDULE 1 — SUB-PROCESSORS

The following Sub-Processors are authorized as of the effective date of this DPA. The list is updated on Tellaro's website (or by direct notice) per Section 4.2.

Sub-Processor	Purpose	Location
H&A Security Solutions, LLC d/b/a Tellaro (self-hosted infrastructure)	Hosting, storage, and processing of Customer Data on Tellaro-owned and -operated infrastructure (no third-party cloud provider for hosting or log storage)	United States
Microsoft Corporation	Email communications via Microsoft 365 (operational and support correspondence)	United States
PagerDuty, Inc.	Operational alerting and on-call notification routing for Tellaro internal teams (may include alert metadata)	United States
Zendesk, Inc.	Customer support ticketing and case management	United States
SentinelOne, Inc.	Endpoint detection and response (only when SentinelOne licensing is purchased)	United States

Notes: Tellaro self-hosts its SaaS Platform on Tellaro-owned and -operated infrastructure; no third-party cloud provider acts as a hosting Sub-Processor. Tellaro VMS (managed vulnerability scanning) is delivered using Tenable Nessus software licensed and operated by Tellaro and does not involve Tenable as a Sub-Processor of Customer Personal Data. Microsoft, PagerDuty, and Zendesk receive limited operational

data and not the bulk of Customer security telemetry; their access to Customer Personal Data is incidental and bounded by the purpose described above.

SCHEDULE 2 — TECHNICAL AND ORGANIZATIONAL MEASURES

- Encryption: TLS 1.2+ for data in transit; AES-256 (or equivalent) for data at rest.
- Access Control: Role-based access, least privilege, multi-factor authentication for all production access.
- Logging and Monitoring: Production access and significant events are logged and monitored.
- Personnel Security: Background checks, confidentiality obligations, and security training.
- Vulnerability Management: Regular vulnerability scanning, patching, and dependency monitoring.
- Incident Response: Documented incident-response plan with defined roles and escalation paths.
- Business Continuity: Backups, redundancy, and documented recovery procedures.
- Vendor Management: Security review of Sub-Processors before engagement and periodically thereafter.
- Compliance: SOC 2 Type II audit (or equivalent) maintained on an annual basis.

SCHEDULE 3 — STANDARD CONTRACTUAL CLAUSES, POPULATED ANNEXES

A. Module Selection.

Module Two of the EU SCCs (Controller to Processor) applies where Customer acts as a Controller of Customer Personal Data. Module Three of the EU SCCs (Processor to Sub-Processor) applies where Customer is itself a Processor for an upstream Controller. The optional clauses are selected as follows:

- Clause 7 (Docking Clause): Not selected.
- Clause 9 (Sub-Processors): Option 2 — General Written Authorization, with the notice period set forth in Section 4.2 of this DPA (30 days).

- Clause 11 (Redress): Optional independent dispute resolution body language NOT selected.
- Clause 17 (Governing Law): Republic of Ireland (for transfers under Module Two/Three from EEA).
- Clause 18 (Choice of forum and jurisdiction): Republic of Ireland (for EEA transfers); United Kingdom courts (for UK-Addendum transfers).

B. Annex I — Description of the Transfer.

(I.A) Parties:

- Data exporter: Customer (as identified on the applicable Order Form) — role: Controller (or Processor for upstream Controller).
- Data importer: H&A Security Solutions, LLC d/b/a Tellaro, 12178 N 1450th Street, Effingham, Illinois 62401, USA — role: Processor (or Sub-Processor where Customer is a Processor).

(I.B) Description of Transfer:

- Categories of data subjects: Customer's employees, contractors, end users, and other persons whose data is captured in Customer security telemetry submitted to the Service.
- Categories of personal data: identifiers, online identifiers, device identifiers, network and security telemetry, user activity data, alerts and case data, and any personal data Customer chooses to submit.
- Sensitive data: Customer is responsible for not submitting special categories of data or sensitive data unless reasonably necessary for security operations.
- Frequency of transfer: continuous, for the duration of the Subscription Term or License Term.
- Nature of processing: hosting, storage, parsing, normalization, correlation, alerting, dashboarding, retrieval, and (where Add-Ons are selected) human review and enrichment.
- Purpose: provision of the Service to Customer.
- Retention: per the retention tier on the applicable Order Form, plus the post-termination data-export window.

(I.C) Competent Supervisory Authority: per Clause 13 of the EU SCCs, the supervisory authority of the EEA member state in which the data exporter is established (or, if the data exporter is not established in the EEA, the supervisory authority of the EEA member state in which the EU Representative is established).

C. Annex II — Technical and Organizational Measures.

The technical and organizational measures applicable to the transfer are set forth in Schedule 2 of this DPA, which is incorporated into Annex II by reference.

D. Annex III — List of Sub-Processors.

The list of authorized Sub-Processors is set forth in Schedule 1 of this DPA, which is incorporated into Annex III by reference.

E. UK Addendum.

For transfers from the United Kingdom, the parties incorporate by reference the UK International Data Transfer Addendum to the EU SCCs (Version B1.0, as may be updated by the UK Information Commissioner). Tables 1–4 of the UK Addendum are populated as follows: Table 1 — parties as in Annex I.A above; Table 2 — Module 2 or Module 3 EU SCCs as selected in Section A above, with the Annexes as completed in Sections B–D above; Table 3 — appendix information per Sections B, C, and D above; Table 4 — neither party may end the UK Addendum as set out in Section 19 thereof.