DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") applies to the Processing of Customer Personal Data (defined below) by the Parties in connection with products and services (the "**Services**") provided under the Agreement.

1. Definitions

1.1. In this Addendum, the following capitalized terms will have the meanings set out below:

(a) "**Agreement**" means the existing Software Services Agreement, order form, or other written agreement between Magnet and Customer pursuant to which Magnet provides the Services to Customer, including any exhibits, statements of work, addenda, and amendments thereto (including this Addendum).

(b) "**Customer Personal Data**" means any Personal Data that is provided by Customer and/or Processed by Magnet on behalf of Customer, pursuant to Magnet's performance of the Services under the Agreement.

(c) "**Data Protection Laws**" means any data protection, privacy, or security laws that may be applicable to Magnet's Processing of Customer Personal Data under the Agreement, including (without limitation) (a) United States federal and state laws and regulations relating to privacy or security, such as the California Consumer Privacy Act as amended by the California Privacy Rights Act ("**CCPA**"); (b) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); and (c) the United Kingdom's General Data Protection Regulation.

(d) "**Data Subject**" means an identified or identifiable living individual to whom the Customer Personal Data relates. For clarity, "Data Subject" also means "Consumer" as such term is defined under applicable Data Protection Laws.

(e) "**Personal Data**" means any information relating to an identified or identifiable living individual, including (without limitation) any information defined as "personal data," "personal information" or an equivalent term under applicable Data Protection Laws.

(f) "**Subprocessor**" means another Processor engaged by Magnet to assist in Magnet's provision of the Services to Customer that Processes Customer Personal Data on behalf of Magnet.

(g) "**Third Country**" means a country or territory that is (a) outside the EEA (for Customers located in an EEA member country); or (b) outside the UK (for Customers located in the UK).

1.2. The terms "**Business**," "**Controller**," "**International Organization**," "**Process**" (and its derivatives), "**Processor**," "**Sell**," "**Share**," and "**Service Provider**" each have the meanings set out in the relevant Data Protection Laws.

1.3. Capitalized terms used but not otherwise defined in this Addendum will have the meanings set out in the Agreement.

2. Processing of Customer Personal Data

2.1. Except where otherwise expressly set forth herein, the Parties agree that Customer is the Controller (and Business) and that Magnet is a Processor (and Service Provider) with respect to the Processing of Customer Personal Data to provide the Services. **Schedule A** to this Addendum sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Customer Personal Data, and the categories of Data Subjects. Customer is responsible for the accuracy, quality,

and legality of the Customer Personal Data it provides to Magnet, and the means by which it acquires and uses Customer Personal Data, including in connection with the Services.

2.2. Each Party will comply with their respective obligations under applicable Data Protection Laws. Customer shall instruct Magnet to process Customer Personal Data in a manner consistent with Data Protection Laws.

2.3. Customer represents and warrants that (a) it will use the Services solely as permitted under the Agreement; (b) it has the authority and right to enter into this Addendum; and (c) it has the authority and right, and all required lawful permission(s), to unlock any Device(s) in Customer's possession, custody, or control; to access and otherwise Process the Customer Personal Data stored on or otherwise accessible within or through such Device(s); and to provide such Customer Personal Data to the Services on behalf of itself, and/or to permit Magnet to do any of the foregoing. Customer warrants and covenants it will at no time unlock or access Devices, Process Customer Personal Data, or instruct Magnet to Process Customer Personal Data in violation of applicable laws. Customer further represents and warrants that it will ensure it has obtained all required permission(s) to access and Process, and to permit Magnet to collect, access, use, store, transfer, and otherwise Process, Customer Personal Data as set forth under the Agreement and this Addendum, such as a court order, lawful governmental or law enforcement request(s), other legal process, or lawful law enforcement powers of investigation, in each case relating to each Data Subject whose Personal Data is accessed or otherwise Processed by Customer and/or Magnet in connection with the Product or the Services. Customer will, upon Magnet's request, provide Magnet with written confirmation of such permission.

2.4. Magnet will Process Customer Personal Data only for the purposes specified in **Schedule A** hereto and in accordance with the documented instructions of Customer. Customer hereby instructs Magnet to Process Customer Personal Data (a) for the purposes specified in Schedule A, including to provide the Services; (b) as permitted by applicable law; (c) in accordance with any settings or configurations applied or provided by Customer or its Authorized Users within the Product or the Services; (d) to engage Subprocessors as permitted hereunder; and (e) as further instructed by Customer in writing. Customer shall ensure that its acts or omissions, including in relation to any instructions to Magnet or Processing of Customer Personal Data, do not cause Magnet to breach Data Protection Laws.

2.5. For Customer Personal Data that is subject to the CCPA, Magnet shall not (a) Sell or Share Customer Personal Data; (b) retain, use or disclose Customer Personal Data outside Magnet's direct business relationship with Customer; or (c) combine Customer Personal Data with Personal Data received from other sources. Magnet will inform Customer if Magnet believes it is unable to comply with the CCPA, permit Customer to suspend any unauthorized Customer Personal Data Processing, and cooperate with Customer to remediate any unauthorized Customer Personal Data Processing so that it is compliant with the CCPA again.

3. Cross-Border Transfers of Personal Data

3.1. The Parties acknowledge and agree that, as of the Effective Date, Customer Personal Data originating from the European Economic Area ("**EEA**") or United Kingdom ("**UK**") transferred by Magnet outside of the EEA and/or UK to a Third Country or International Organization not deemed adequate by the European Commission is subject to the terms of the Standard Contractual Clauses Module Two (Controller to Processor) as incorporated herein by reference.

a) Restricted Transfers. Customer will operate as a Controller and Magnet will operate as Processor, Processing Customer Personal Data only as necessary for the limited and specified purposes identified in the Agreement, and in accordance with at least the same level of protection as is required under the applicable Data Protection Laws. To the extent Magnet Processes any Customer Personal Data subject to the EU GDPR or UK GDPR under the Agreement, any such transfer will be subject to the EU SCCs or UK IDTA, as applicable and as set forth under Section 3(b) and 3(c) below. Where such

international transfers may be necessary to perform under the Agreement, Customer authorizes Magnet and its Subprocessors to make international transfers of Customer Personal Data in accordance with this DPA so long as applicable Data Protection Laws for such transfers are complied with. Customer shall notify Magnet prior to disclosing Personal Data whether any Personal Data subject to the EU GDPR or UK GDPR will be Processed by Magnet.

b) Transfers from the EEA. With respect to Customer Personal Data transferred from the European Economic Area ("EEA"), the EU SCCs incorporated herein shall apply, form part of this DPA, and take precedence over the rest of this DPA as set forth in the EU SCCs. They will be deemed completed as follows:

i) Where Customer is a data exporter and controller, and Magnet is a data importer and processor, Module 2 shall apply.

ii) Clause 7, the "Docking Clause (Optional)", will be deemed omitted.

iii) Under Clause 9 (Use of sub-processors), the Parties select Option 2 (general written authorization), and the time period for prior notice of addition or replacement of Sub-Processors will be as set forth in Section 6 of this DPA.

iv) Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

v) Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law France.

vi) Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of France.

vii) Annexes I and II are appended to this DPA.

viii) By entering into this DPA, the Parties are deemed to be signing the EU SCCs and its applicable Annexes. The most current version of the EU SSCs can be found at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

c) Transfers from the UK. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any EEA jurisdiction) governs the international nature of the transfer and a data transfer mechanism is required, the applicable UK IDTA forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK IDTA, unless the United Kingdom issues updates to the UK IDTA that, upon notice from Customer, will control. Undefined capitalized terms used in this provision shall mean the definitions in the UK IDTA.

i) For transfers from the UK, the UK Addendum, template Addendum B.1.0 issued 2 February 2022 will be deemed executed. Where applicable, the UK Addendum shall be deemed completed as follows:

(1) Table 1 of the UK Addendum: (1) the Parties' details shall be the Parties and their Affiliates to the extent any of them is involved in such transfer, including those set forth in Annex 1; (2) the Key Contact shall be the contacts set forth in Annex 1.

(2) Table 2 of the UK Addendum: The version of the Approved EU SSCs which are incorporated by reference herein apply.

(3) Table 3 of the UK Addendum: (1) List of Parties (IDTA Annex 1.A) is outlined in Annex 1; (2) Description of Transfer (IDTA Annex 1.B) is outlined in Annex 1; (3) Technical and

Organisational Measures (IDTA Annex II) are outlined in Schedule B; List of Subprocessors (IDTA Annex III) are outlined in Schedule A. .

(4) Table 4 of the UK Addendum: Neither Party may end this DPA as set out in Section 19 of the UK Addendum.

(5) By entering into this DPA, the Parties are deemed to be signing the UK Addendum and its applicable Tables and Appendix Information.

d) Statutory Revisions to the EU SCCs or UK IDTA. In the event that the EU GDPR or UK GDPR require the use of revised standard contractual clauses applicable to this DPA, such revised standard contractual clauses shall automatically be deemed to replace the EU SCCs and/or UK IDTA, as applicable, without the need for any further action, unless Magnet otherwise informs Customer. Transfers From Switzerland. With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, references to the EU GDPR in Clause 4 of the EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

e) Transfers from the Dubai International Financial Centre ("DIFC"). Personal data that is subject to DIFC data protection laws ("DIFC Personal Data") shall be governed by these Standard Contractual Clauses. For exported personal data that is subject to DIFC data protection laws, the Data Protection Law DIFC Law No. 5 of 2020, as amended, shall govern such SCCs for the purposes of DIFC Personal Data. The Commissioner of Data Protection for the DIFC shall be the supervisory authority for DIFC Personal Data.

3.2. If Customer Personal Data must be transferred, does not fall under the obligations of Clause 3.1, and is subject to other specific transfer requirements or mechanisms, Customer shall inform Magnet of the restrictions and obligations. The Parties agree to work together in good faith to amend this Addendum or enter into any additional clauses required to permit a compliant transfer of Customer Personal Data to Magnet.

3.3. Magnet may transfer Customer Personal Data onward to another party subject to appropriate safeguards and/or transfer mechanisms that are in compliance with Data Protection Laws.

4. **Personnel**. Magnet will ensure that any Magnet personnel authorized to Process Customer Personal Data have committed themselves to an appropriate duty of confidentiality or are under an appropriate statutory obligation of confidentiality.

5. **Security**. Magnet will, in relation to the Customer Personal Data, implement appropriate technical and organizational measures, as set forth in **Schedule B** to this Addendum, which are designed to ensure a level of security appropriate to the risks presented by Magnet's Processing of Customer Personal Data. In case of a security incident affecting Customer Personal Data, Magnet will take prompt steps to remediate the security incident and will provide notice to Customer without undue delay, and in any event, within seventy-two (72) hours after becoming aware of such security incident. Magnet will provide Customer with reasonable information necessary for Customer to be able to comply with Customer's notice requirements to Data Subjects and/or regulators and will reasonably cooperate with Customer's need for assistance in responding to the security incident.

6. **Subprocessing**. Customer expressly consents to Magnet's engagement of Subprocessors. The Subprocessors applicable to Customer Personal Data may depend on Customer's location and the

Product(s) purchased and/or licensed. Please see **Schedule A** of this Addendum. Customer agrees that Magnet may engage further Subprocessors subject to the following requirements:

6.1. Magnet will provide Customer with notice of a new Subprocessor Processing Customer Personal Data. Upon receipt of such notice, Customer may reasonably and in good faith object to the new Subprocessor in writing within fifteen (15) calendar days. The Parties agree to work together in good faith to resolve any objection.

6.2. Magnet will enter into a written contract with Subprocessors that include contractual terms requiring an equivalent level of protection for Customer Personal Data as those set out in this Addendum and will remain liable to Customer for the performance of each Subprocessor's Processing of Customer Personal Data in the performance of the Services.

7. **Reasonable Assistance.** Upon Customer's reasonable request and to the extent that such assistance does not require Magnet to access Customer Personal Data it does not access in the ordinary course of providing the Services, Magnet will provide reasonable assistance to Customer to comply with the provisions in Data Protection Laws governing Data Subject rights, privacy or data protection assessments and/or regulatory consultations.

8. **Deletion or Return of Customer Personal Data**. During the provision of the Services, Customer and/or Customer's Authorized Users may delete Customer Personal Data from the Services. Following expiration or termination of the Agreement, or otherwise at the end of the provision of the Services, Customer will have sixty (60) calendar days to retrieve Customer Personal Data from the Services, after which time Magnet will delete the Customer Personal Data. On Customer's request, Magnet will confirm in writing that Customer Personal Data has been deleted. This Addendum shall remain in effect until all Customer Personal Data has been destroyed.

9. **Audit Rights.** Upon Customer's written request and no more than once annually, Magnet shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of Magnet) information necessary to demonstrate Magnet's compliance with its obligations under this Addendum and/or Data Protection Laws. As an alternative, and at its sole discretion, Magnet may (i) engage a qualified and independent third party to evaluate Magnet's technical and organizational security measures, which Customer will agree to accept a summary of unless more detailed information is required to comply with Data Protection Laws; or (ii) provide a summary of an evaluation from an independent third party that has been conducted in the twelve (12) months preceding Customer's request, which Customer will agree to accept unless more detailed information is required to comply with Data Protection Laws. Any information provided to Customer under this Section 9 is Magnet's Confidential Information.

10. **Changes in Data Protection Laws**. If any amendment to this Addendum is required as a result of a change or update in Data Protection Laws, then Magnet shall provide updates to this Addendum accordingly. Changes shall be strictly in accordance with the requirements of Data Protection Laws.

SCHEDULE A

to the Data Processing Addendum

Details of Processing of Customer Personal Data

1. **Purposes of Processing; Processing Operations**

The nature and purpose of the Processing of Customer Personal Data include:

The provision of the Services in accordance with the Agreement and this Addendum.

2. **Customer Personal Data**

a. Types of Personal Data

We collect a limited amount of personal data in connection with our software and support services. The following categories of personal data are collected:

- Business contact and payment information
- Technical or internet information for license activation (e.g., UUID, username, computer and domain name server information)
- Information consistent with our Cookie Policy;
- Other information voluntarily provided by you while obtaining support services.

Please see our Privacy Policy for more information. Our Cookie Policy and Privacy Policy can be found at www.magnetforensics.com/legal.

b. Data Subjects

The categories of Data Subjects to whom Customer Personal Data relates include:

- Customer's personnel
- Other Data Subjects whose Personal Data Customer collects and Processes pursuant to the Services

3. **Duration of Processing**

Continuous for duration of the Agreement, plus the period from the expiry of the Agreement until the return or deletion of all Customer Personal Data by Magnet in accordance with the Agreement (including this Addendum), Customer's instructions, and applicable law.

4. **Approved Subprocessors**

The Subprocessors applicable to Customer Personal Data may depend on Customer's location and the product(s) Customer has purchased and/or licensed. Please speak to your account representative or contact us as described herein for more information.

a. **Amazon Web Services, Inc.**
Services provided: Cloud hosting for Customer Personal Data and infrastructure for Services

b. **SalesForce**
Services provided: Customer management, product documentation, project management, documentation feedback, and product training.

c. **Gainsight PX**
Services Provided: product usage data for certain products.

d. **Gainsight CS**
Services Provided: customer management for certain products.

e. **Flexera**
Services Provided: product licensing.

f. **Skilljar**
Services Provided: product training.

g. **Smartsheet**
Services Provided: project management.

h. **Slack**
Services Provided: project management.

i. **JIRA**
Services Provided: case management.

j. **SharePoint**
Services Provided: project management.

k. **Mailchimp**
Services Provided: marketing, licensed application functionality

l. **MailGun**
Services Provided: marketing, licensed application functionality

m. **SendGrid**
Services Provided: marketing, licensed application functionality

n. **Okta**
Services Provided: SSO, marketing and product planning purposes, sign-on functionality

o. **Zoho Forms**
Services Provided: surveys, product feedback requests

p. **Aha!**
Services Provided: roadmap management, Ideas portal.

SCHEDULE B

to the Data Processing Addendum

Technical and Organizational Measures

1. Magnet has implemented and will maintain a comprehensive, written information security program. One or more designated qualified individuals is/are responsible for maintaining Magnet's information security program. Magnet will regularly review the information security program to identify and assess reasonably foreseeable internal and external risks to the privacy, security, and/or integrity of any electronic, paper, or other records containing Customer Personal Data and to ensure that Magnet's information security program continues to comply with applicable Data Protection Laws.

2. Magnet's relevant information security program (with regard to the Customer Personal Data) materially conforms with ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. In addition, Magnet will undergo a SOC 2, Type II report on controls relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy of its relevant systems and processes, conducted by a qualified, independent, professional audit firm. Upon request, Magnet will permit Customer to review the results from any such audit reports or assessments (which shall be Magnet's Confidential Information), as relevant to the Customer Personal Data.

3. Any Processing of Customer Personal Data will take place on information processing systems for which commercially reasonable technical and organizational measures designed for protecting Customer Personal Data have been implemented. Magnet will maintain reasonable and appropriate technical, physical, and administrative measures designed to protect Customer Personal Data under its possession or control against unauthorized or unlawful Processing or accidental loss, destruction, or damage in accordance with the applicable Data Protection Laws, taking into account the harm that might result from unauthorized or unlawful Processing or accidental loss, destruction, or damage and the sensitivity of the Customer Personal Data.

4. Magnet will (a) take reasonable steps to ensure the reliability of employees, temporary workers, contractors, and other personnel (collectively "**Personnel**") having access to Customer Personal Data; (b) limit access to Customer Personal Data to those Personnel who have a business need to have access to such Customer Personal Data and have received reasonable and appropriate privacy and security training; and (c) conduct background checks for employees and contractors with responsibilities for or access to Customer Personal Data, to the extent permissible under applicable law.

5. **Minimum Controls**. Without limiting any other obligations herein, the following security controls will be implemented:

   (a) policies, procedures, and processes to manage the security risks related to Processing of Customer Personal Data are documented, understood, reviewed, and updated periodically;

   (b) devices, systems, facilities, and other assets ("**Assets**") that access, store, and Process Customer Personal Data, as well as those that are material to the provision of the Services to the Customer under the Addendum are identified and managed;

   (c) physical access to Assets is managed and controlled, including measures to prevent and detect unauthorized access to Assets (including facilities), and access to Assets is limited to authorized users;

   (d) security risk assessments are performed to identify and assess reasonably foreseeable internal and external security risks;

   (e) remote access by Personnel and others to Assets is restricted and securely managed with multi-factor authentication;

(f) Customer Personal Data and related records are identified, and access is managed to protect the confidentiality, integrity, and availability of such data;

(g) monitoring tools are in place to allow for the review of unauthorized activity;

(h) electronic and paper records containing Customer Personal Data are securely destroyed in accordance with secure destruction policies and procedures;

(i) appropriate technical security solutions are implemented and managed to protect the confidentiality, integrity, and availability of Customer Personal Data;

(j) critical operating system and software security patches will be installed in a timely manner on all devices used to Process Customer Personal Data, and identified security-related fixes will be promptly installed;

(k) anti-malware software will be installed and configured to check for updates on a regular basis on all devices used to Process Customer Personal Data;

(l) maintenance and repair of information system components is performed in a controlled and secure manner;

(m) Magnet's network and Assets are monitored to detect vulnerabilities, threats, anomalous or unauthorized activity, and other potential cyber security events (collectively, "**Events**") in timely manner;

(n) Customer Personal Data will not be stored on any portable or removable media;

(o) Customer Personal Data will not be stored or used in test or other non-production environments; and

(p) incident response processes and procedures are maintained and executed, to ensure timely response to detected Events, and the following activities take place according to such established processes and procedures: (i) Events are investigated, understood, and categorized; (ii) activities are performed to contain an Event, mitigate its effects, and address any remaining threat or vulnerability; (iii) Assets and Customer Personal Data affected are restored, and other appropriate mitigating actions are taken; (iv) response and recovery activities are documented; and (v) policies and procedures are routinely reviewed and updated to incorporate lessons learned and address potential threats and vulnerabilities.

6. **Encryption and Infrastructure Protection**. Customer Personal Data, including Customer Personal Data on portable devices and backup media, will be encrypted in transmission and at rest, using industry-standard cryptographic techniques and secure management of keys.

7. **System Authentication and Authorization**. Access to Customer Personal Data will be subject to secure user authentication protocols, including controls around user IDs, other identifiers, passwords, biometrics, authentication token devices, active account log-in procedures, log records that record access attempts, and blocking after multiple unsuccessful log-in attempts.

   (a) Review of user access rights to systems containing Customer Personal Data will be conducted regularly.

   (b) Magnet will maintain electronic logs of persons accessing Customer Personal Data depicting the details of the access and transactional changes made. Such electronic logs must be provided to Customer for inspection upon reasonable request.

8. **Business Continuity**. Magnet will have in place appropriate business continuity and disaster recovery

procedures for its business (the "**Business Continuity Plan**") to ensure the continued performance of its obligations under the Addendum and operational resilience generally, and will develop, test and update the Business Continuity Plan regularly, in accordance with good industry practice.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: Customer, as set out in the Agreement

Address: Customer's address, as set out in the Agreement

Contact person's name, position and contact details: Customer's contact, as set out in the Agreement

Activities relevant to the data transferred under these Clauses: Provide Personal Data to receive the Services

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: **Magnet Forensics USA Inc.**

Address: 2250, Corporate Park Dr #130, Herndon, VA 20171

Contact person's name, position and contact details: dpo@magnetforensics.com

Activities relevant to the data transferred under these Clauses: Provide the Services

Signature and date:

Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

See Annex I

Categories of personal data transferred

See Annex I

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Annex I

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Periodic

Nature of the processing

Collection, organization, storage, provision of access, restriction, erasure and destruction

Purpose(s) of the data transfer and further processing

For provision of the Services

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Annex I

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subprocessors will process Personal Data in accordance with the subject matter, nature, and duration of the Controller's processing.

C. **COMPETENT SUPERVISORY AUTHORITY**

The supervisory authority of one of the Member States in which the data subjects whose Personal Data is transferred under these Clauses are located shall act as competent supervisory authority.

ANNEX II

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

The technical and organizational measures are set out in Schedule B.